La Convention 108 du Conseil de l'Europe pour la protection des données, 40 ans et après ?

De Terwangne, Cecile

Published in:
Politeia

Publication date:
2021

Document Version
le PDF de l'éditeur

Les Cahiers de l'Association Française des Auditeurs
de l'Académie Internationale de Droit Constitutionnel

Politeia

Prochain dossier constitutionnel :
Réanimer la démocratie, quels remédes ? (automne 2021)
Courriel : redaction@revue-politeia.com - Site web : http://www.revue-politeia.com

Prix public : 45 euros

ISSN : 1628-6782

Les Cahiers de l'AFAAIDC

Politeia

Numéro 39
Printemps
2021

Les Cahiers de l'Association Française des Auditeurs
de l'Académie Internationale de Droit Constitutionnel

Politeia

20 ANS de *Politeia*

Le Conseil de l'Europe, 70 ans et après ?

Numéro 39 **Printemps 2021**

Revue semestrielle de Droit constitutionnel comparé
publiée sous le haut patronage de l'Académie Internationale de Droit Constitutionnel,
de l'Association Française des Auditeurs de l'Académie Internationale de Droit Constitutionnel
et avec le concours du Centre de Recherches et de Documentation Européennes et Internationales (CRDEI)
et de l'Université de Bordeaux

Les Cahiers de l'Association Française des Auditeurs
de l'Académie Internationale de Droit Constitutionnel

*P*OLITEIA

■ Numéros parus

- Numéro 1 (printemps 2001)
- Numéro 2 : Communautés et communautarisme (printemps 2002)
- Numéro 3 : Droit à la vie, droit à la mort, un droit constitutionnel ? (printemps 2003)
- Numéro 4 : L'effectivité de la norme constitutionnelle (automne 2003)
- Numéro 5 : Droit constitutionnel et droit pénal (printemps 2004)
- Numéros 6 et 7 : Souverainisme, nationalisme, régionalisme (I et II) (2004)
- Numéro 8 : Europe et Constitution (automne 2005)
- Numéros 9 et 10 : Liberté d'expression et démocratie (I et II) (2006)
- Numéro 11 : La campagne présidentielle de 2007 : quels débats constitutionnels ? (printemps 2007)
- Numéro 12 : Les formes d'État aujourd'hui (automne 2007)
- Numéro 13 : Constitution et traité de Lisbonne (printemps 2008)
- Numéro 14 : Images croisées de la présidence américaine (automne 2008)
- Numéros 15, 16, 17 : La réforme des institutions françaises (I, II, III) (2009-2010)
- Numéro 18 : Les nouveaux aspects du constitutionnalisme (automne 2010)
- Numéro 19 : Égalité - Parité : une nouvelle approche de la démocratie ? (printemps 2011)
- Numéro 20 : Le droit constitutionnel calédonien (automne 2011)
- Numéro 21 : Le vote à l'écran (printemps 2012)
- Numéro 22 : Droit constitutionnel et droits externes (automne 2012)
- Numéro 23 : La fonction présidentielle sous le quinquennat Sarkozy (printemps 2013)
- Numéro 24 : Les populismes d'hier et d'aujourd'hui (automne 2013)
- Numéro 25 : Souveraineté de l'État et supranationalité normative. Les droits européens (printemps 2014)
- Numéro 26 : Modèles et modélisation en droit constitutionnel. Approches classiques, nouvelles pratiques (automne 2014)
- Numéro 27 : Quelle démocratie européenne ? (printemps 2015)
- Numéro 28 : Violence et action politique (automne 2015)
- Numéro 29 : Laïcité et démocratie (printemps 2016)
- Numéro 30 : Les droits et libertés fondamentaux, horizon indépassable du droit constitutionnel ? (automne 2016)
- Numéro 31 : Les métamorphoses des droits fondamentaux à l'ère du numérique (printemps 2017)
- Numéro 32 : Ordres constitutionnels, international et européen (automne 2017)
- Numéro 33 : L'Union européenne, « *in/out* » (printemps 2018)
- Numéro 34 : La Constitution économique (automne 2018)
- Numéro 35 : La réforme de la zone euro, entre parlementarisation des choix et automatisation des règles (printemps 2019)
- Numéro 36 : Maturité et utilité de la Constitution de 1958 dans le contexte européen (automne 2019)
- Numéro 37 : La constitutionnalisation de la santé en Italie et en France (printemps 2020)
- Numéro 38 : Les amendements budgétaires en droit comparé (automne 2020)
- Numéro 39 : Le Conseil de l'Europe, 70 ans et après ? (printemps 2021)

■ Numéro à paraître

- Numéro 40 : Réanimer la démocratie, quels remèdes ? (automne 2021)

*P*OLITEIA

■ Chroniques constitutionnelles

Jean Mermoz Bikoro, *La fonction constituante du peuple dans le nouveau constitutionnalisme des États d'Afrique noire francophone*
Stéphane Caporal-Greco, *La liberté d'expression des militaires*
El Maamoun Fikri, *La rationalisation du parlementarisme, approche comparée France-Maroc*
Ayme Elouma Lazare II, *La participation des assemblées parlementaires d'Afrique noire à la politique étrangère : le cas du Parlement camerounais*
Antoine Ploux, *La motivation comme remède à la crise de confiance dans le droit !*
Éric Simo, *Le statut constitutionnel d'ancien chef d'État en Afrique noire francophone*
Serge Surin, *Le contrôle de constitutionnalité a-t-il vraiment tué la loi rousseauiste ? Réflexions autour de la jurisprudence selon laquelle "la loi votée […] n'exprime la volonté générale que dans le respect de la Constitution"*

■ Chroniques bibliographiques

Manon Decaux, *À propos de* Réclamer en démocratie, *sous la direction de Dominique Rousseau*
Julien Giudicelli, *À propos de* Démocratie : l'héritage politique grec, d'Yves Mény
Tanguy Pasquiet-Briand, *À propos de* La notion de constitution dans la doctrine constitutionnelle de la Troisième République, *sous la direction d'Armel Le Divellec*

La Chronique de Petri, le Souletin de Etchebar. *Ainsi fait, fait, fait Macron, la p'tite Macronnette, … avec ses Macronades et autres Macronner…!*

LA CONVENTION 108 DU CONSEIL DE L'EUROPE POUR LA PROTECTION DES DONNÉES, 40 ANS ET APRÈS ?

Par Cécile DE TERWANGNE

Professeur à l'Université de Namur (Belgique)
Directrice de recherche au CRIDS
(Centre de recherche Information, Droit et Société)

SOMMAIRE

Née à Strasbourg au sein du Conseil de l'Europe, le 28 janvier 1981, la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a quarante ans en 2021. Quarante ans, c'est l'heure du bilan. La crise de la quarantaine signifie généralement l'envie de changer les choses pour l'avenir sans faire nécessairement *tabula rasa* du passé. C'est précisément le sort qui a été réservé à la Convention 108 qui a subi une vaste opération de modernisation. Une version révisée de la Convention a été adoptée le 18 mai 2018[1] et ouverte à la signature le 10 octobre de la même année.

[1] protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), signé à Elseneur, 18 mai 2018, disponible à l'adresse : https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65c0. Sur ce nouveau texte, voy. C. DE TERWANGNE, « Privacy and data protection in Europe: Council of Europe and European Union legislations », *in Research Handbook on Privacy and Data Protection Law*, London, Edward Elgar, 2021 (à paraître).

Le travail de modernisation a été mené dans un premier temps par le Comité consultatif de la Convention (T-PD) et poursuivi par le Comité *ad hoc* sur la protection des données (CAHDATA) intégrant des représentants de l'Union européenne aux côtés des représentants des États Parties à la Convention. L'objectif était de permettre de répondre aux nouveaux défis issus des développements technologiques et sociétaux spectaculaires survenus depuis l'adoption de la Convention. Les réponses juridiques pour protéger les individus en 1981, à une époque qui ne connaissait ni Internet, ni réseaux sociaux, ni *Big data*, ni objets connectés, ni géolocalisation, ni intelligence artificielle, se sont révélées insuffisantes dans le monde devenu interconnecté et où les données à caractère personnel sont devenues l'objet de toutes les convoitises.

L'heure de la révision avait d'ailleurs également sonné pour l'autre instrument juridique européen en la matière, la directive 95/46 de l'Union européenne. Cette directive a laissé place le 25 mai 2018 au très médiatique règlement général sur la protection des données (RGPD)[2]. Ce calendrier conjoint d'*aggiornamento* des deux principaux instruments juridiques européens relatifs à la protection des données, ainsi que l'association de représentants de l'Union européenne aux discussions portant sur la modernisation de la Convention 108, ont permis de nourrir réciproquement les réflexions entre Strasbourg et Bruxelles[3]. Une attention particulière a été accordée à la cohérence entre les deux textes afin d'éviter que les États liés de part et d'autre ne soient tenus par des engagements contradictoires. RGPD et Convention 108 modernisée s'inscrivent donc dans la continuité des textes qui les précèdent, la directive 95/46 ayant proclamé « *que les principes de la protection des droits et des libertés des personnes, notamment du droit à la vie privée, contenus dans la présente directive précisent et amplifient ceux qui sont contenus dans la convention, du 28 janvier 1981, du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* »[4].

Le résultat du travail de modernisation de la Convention fait l'objet de l'analyse présentée dans les pages qui suivent. Le propos portera sur le texte du protocole d'amendement du 18 mai 2018, baptisé par les services du Conseil de l'Europe, dans un souci de communication efficace, la « Convention 108+ », éclairé des indications fournies dans le rapport explicatif de cette Convention 108 modernisée. Il est à noter que, fait peu commun, le Comité des ministres a entériné le rapport explicatif. Dès lors, « *le rapport explicatif fait partie du contexte au vu duquel la signification de certains termes employés dans la Convention doit être*

[2] Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive n° 95/46/CE (règlement général sur la protection des données), *JOUE* L 119/1, 4 mai 2016.

[3] C. DE TERWANGNE et S. KWASNY, « La protection des données à l'ère du numérique : la Convention 108+, parente et nécessaire alliée du RGPD », *Dalloz IP/IT*, 2020, n° 11, p. 607-611.

[4] Considérant 11 de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *JOCE* L 281, 23/11/1995.

établie (article 31, paragraphes 1 et 2 de la Convention de Vienne sur le droit des traités des Nations unies). »[5]

I. – INSTRUMENT JURIDIQUE CONTRAIGNANT DE PORTÉE UNIVERSELLE

La Convention 108, dans sa version originale de 1981, a été ratifiée par les quarante-sept États membres du Conseil de l'Europe. La Convention a ainsi servi de fondation aux régimes de protection des données à caractère personnel de l'ensemble des États du continent européen (à la seule exception de la Biélorussie, non-membre du Conseil de l'Europe).

La Convention est, à ce jour, l'unique texte juridiquement contraignant à vocation universelle en matière de protection des données. Selon les termes du Préambule de la Convention 108+, les États signataires de ce texte reconnaissent « *la nécessité de promouvoir les valeurs fondamentales du respect de la vie privée et de la protection des données à caractère personnel à l'échelle mondiale, favorisant ainsi la libre circulation de l'information entre les peuples* »[6]. Si les principes de protection des données à caractère personnel proviennent du creuset européen, ils ont indéniablement vocation à porter leurs effets bien au-delà des frontières européennes.

Une des singularités notables de la Convention est en effet qu'elle est ouverte à la signature d'États ne faisant pas partie du Conseil de l'Europe. L'article 23 du texte de 1981 règle l'adhésion de ces États en ces termes : « *1. Après l'entrée en vigueur de la présente Convention, le Comité des ministres du Conseil de l'Europe pourra inviter tout État non-membre du Conseil de l'Europe à adhérer à la présente Convention par une décision prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe et à l'unanimité des représentants des États contractants ayant le droit de siéger au Comité.* » À ce jour, cette procédure a abouti à la ratification de la Convention par (dans l'ordre chronologique) l'Uruguay, Maurice, le Sénégal, la Tunisie, le Cap-Vert, le Mexique, l'Argentine et le Maroc. À l'avenir, lorsque la version modernisée de la Convention sera entrée en vigueur, deux exigences procédurales supplémentaires devront être respectées pour permettre l'adhésion d'un État tiers ou d'une organisation internationale : il faudra recevoir l'avis du Comité conventionnel et obtenir l'accord unanime des Parties à la Convention (qui ne siègent pas toutes au Comité des ministres, celui-ci étant limité aux États membres du Conseil de l'Europe)[7].

---

[5] Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), Rapport explicatif, 18 mai 2018, § 6.

[6] Nos italiques.

[7] Article 27, § 1, de la Convention 108+ : « *Après l'entrée en vigueur de la présente Convention, le Comité des ministres du Conseil de l'Europe pourra, après consultation des Parties à la présente Convention et en avoir obtenu l'assentiment unanime, et à la lumière de l'avis formulé par le Comité conventionnel, conformément à l'article 23.e, inviter tout État non membre du Conseil de l'Europe ou une organisation internationale à adhérer à la présente Convention par une décision prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe, et à l'unanimité des représentants des États contractants ayant le droit de siéger au Comité des ministres.* »

Tout État désireux d'adhérer à la Convention 108 depuis le 10 octobre 2018, date d'ouverture à la signature du protocole d'amendement du 18 mai 2018, ne peut devenir Partie sans adhérer simultanément au protocole[8].

Il est à noter que la Convention 108+ est ouverte à la signature non seulement d'États mais également d'organisations internationales. Ainsi des organisations internationales comme l'Union européenne et le Comité international de la Croix-Rouge (CICR) ont marqué dès le début des travaux de modernisation auxquels ils ont intensément participé, leur intérêt à devenir parties à la Convention modernisée[9].

La Convention 108+ entrera en vigueur le 11 octobre 2023 dans l'hypothèse où le protocole comptera au moins trente-huit Parties à cette date. Si ce n'est pas le cas, elle n'entrera en vigueur que lorsque le protocole sera ratifié par toutes les Parties à la Convention 108. À ce jour (mars 2021), il a été ratifié par 11 États.

II. – LES VALEURS LIÉES À LA PROTECTION DES DONNÉES : LA DIGNITÉ HUMAINE ET L'AUTONOMIE PERSONNELLE

A. – *La dignité humaine*

Le préambule de la Convention 108 dans sa version modernisée affirme solennellement « *qu'il est nécessaire de garantir la dignité humaine ainsi que la protection des droits de l'homme et des libertés fondamentales de toute personne [...]* »[10].

Dès l'entame du nouveau texte donc, on reconnaît la nécessité de garantir la dignité humaine face aux traitements de données à caractère personnel. Il s'agit de rappeler que l'être humain doit demeurer un sujet et non être réduit à un simple objet, qu'il s'agisse d'un objet de déductions algorithmiques, de contrôle ou de surveillance. Le rapport explicatif de la Convention 108+ le dit en ces termes : « *La dignité humaine requiert la mise en place de garanties lors du traitement de données à caractère personnel, afin que les individus ne soient pas traités comme de simples objets.* »[11]

Cette proclamation de la valeur fondamentale de la dignité humaine en entame de la Convention 108+ est sans aucun doute particulièrement nécessaire aujourd'hui face aux décisions automatisées, au recours à l'intelligence artificielle alimentée par les données massives (*Big Data*), à la mise en place de systèmes

[8] Article 36, § 2 du protocole d'amendement.
[9] L'Union européenne espère depuis 1999 être admise à adhérer à la Convention 108, voy. amendement à la Convention STE n° 108 permettant l'adhésion des Communautés européennes : adopté le 15 juin 1999 (amendement jamais entré en vigueur car il nécessitait l'acceptation de toutes les Parties), http://conventions.coe.int/Treaty/fr/Treaties/Html/108-1.htm.
[10] Nous soulignons.
[11] Rapport explicatif de la Convention 108+, § 10.

d'information à grande échelle (tels, pour l'Union européenne, les systèmes SIS, VIS ou Eurodac[12]), *etc.*.

C'est notamment dans l'exigence que le sort d'un individu ne soit pas exclusivement décidé par un logiciel (droit de ne pas être soumis à une décision entièrement automatisée)[13] que se traduira la protection de la dignité humaine.

C'est aussi au nom de la dignité humaine qu'on ne peut admettre n'importe quel traitement de données alors même qu'une entité publique aurait autorisé le traitement en question ou que la personne concernée aurait consenti à voir ses données traitées. Sur ce dernier point, comme le dit le paragraphe 44 du Rapport explicatif de la Convention 108+, « *[l]'expression d'un consentement ne dispense pas de respecter les principes fondamentaux de la protection des données à caractère personnel […] : la proportionnalité du traitement, par exemple, doit toujours être considérée* ». Ce qu'un individu va peut-être être amené à accepter du fait des mauvaises conditions dans lesquelles il donne son consentement ou de n'être pas suffisamment éclairé sur les conséquences à long terme du traitement de ses données ou sur l'impact de tels traitements sur l'ensemble d'une communauté humaine, la société ne doit pas nécessairement l'admettre. La proportionnalité d'un traitement de données implique de prendre en considération l'impact de ce traitement sur les intérêts, droits et libertés des personnes dont les données sont traitées, au titre desquels relève la dignité de ces personnes. Et cette prise en compte peut aussi intervenir alors même que la décision de traiter les données proviendrait d'une autorité publique. Le système de crédit social développé ces dernières années en Chine[14] et impliquant l'attribution à chaque citoyen d'un « score » reposant sur des outils de surveillance globale et de masse offre un exemple de cas dans lequel un système de traitement de données porte excessivement atteinte à la dignité des individus et ne devrait dès lors pas être mis en place. On doit pouvoir contester devant un tribunal ou un organe de recours (voy. *infra*) la mise en œuvre des traitements de données qui portent atteinte à la dignité humaine.

B. – *L'autonomie personnelle, l'autodétermination informationnelle*

Après avoir affirmé la nécessité de garantir la dignité humaine, le préambule de la Convention 108+ poursuit en soulignant la nécessité de garantir également « *la protection des droits de l'homme et des libertés fondamentales de toute personne, et, eu égard à la diversification, à l'intensification et à la mondialisation des traitements des données et des flux de données à caractère personnel, l'autonomie*

[12] Système d'information Schengen ; Système d'information sur les visas ; Système Eurodac pour la comparaison des empreintes digitales des demandeurs de protection internationale et pour l'identification des ressortissants des pays tiers ou apatrides en séjour irrégulier.
[13] Voir *infra*.
[14] R. RAPHAËL et L. XI, « Bons et mauvais Chinois : Quand l'État organise la notation de ses citoyens », *Le Monde diplomatique*, janvier 2019, https://www.monde-diplomatique.fr/2019/01/RAPHAEL/59403.

personnelle, fondée sur le droit de toute personne de contrôler ses propres données à caractère personnel et le traitement qui en est fait »[15].

La Cour européenne des droits de l'homme a expressément reconnu dans son arrêt *Satamedia* de 2017[16] qu'un droit à l'autodétermination informationnelle[17] était attaché au droit à la protection de la vie privée. Elle a ainsi établi que « *[l] a protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article […]. L'article 8 de la Convention consacre donc le droit à une forme d'autodétermination informationnelle, qui autorise les personnes à invoquer leur droit à la vie privée en ce qui concerne des données qui, bien que neutres, sont collectées, traitées et diffusées à la collectivité, selon des formes ou modalités telles que leurs droits au titre de l'article 8 peuvent être mis en jeu.* »[18]

La protection des données est une émanation du droit au respect de la vie privée pris dans la dimension de droit à l'autonomie. C'est le droit pour chacun de déterminer quelles informations le concernant peuvent être communiquées à qui et à quelles fins. C'est le droit de contrôler ses propres données, qu'elles soient intimes et privées ou professionnelles et publiques, qu'il s'agisse de données sensibles ou de données « neutres » pour reprendre les termes de la Cour européenne des droits de l'homme.

III. – LE CHAMP D'APPLICATION DE LA CONVENTION 108+

A. – *Un champ particulièrement large*

La Convention est applicable à toute activité de traitement de données, effectuée tant dans le secteur public que dans le secteur privé. C'est donc

[15] Nous soulignons. Voy. déjà en 1998 : Rés. 1165(1998) de l'Assemblée parlementaire du Conseil de l'Europe sur le droit au respect de la vie privée, adoptée le 26 juin1998 : « *Pour tenir compte de l'apparition des nouvelles technologies de la communication permettant de stocker et d'utiliser des données personnelles, il convient d'ajouter à cette définition [du droit au respect de la vie privée] le droit de contrôler ses propres données* » (nous soulignons).

[16] Cour eur. D.H. [GC], *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, arrêt du 27 juin 2017, req. n° 931/13.

[17] Sur la notion de droit à l'autodétermination informationnelle, voy. A. ROUVROY,Y. POULLET, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel : une réévaluation de l'importance du droit à la protection de la vie privée pour la démocratie », *in* K. BENYEKHLEF, P. TRUDEL (dir.), *État de droit et virtualité*, Montréal, Thémis, 2009, p. 157-222, disponible à l'adresse http://www.crid.be/pdf/public/6050.pdf ; T. LÉONARD, Y. POULLET, « Les libertés comme fondement de la protection des données nominatives », *in* F. RIGAUX (dir.), *La vie privée : une liberté parmi les autres ?*, Bruxelles, Larcier, 1992, p. 231 et s. ; C. DE TERWANGNE, « La difficile application de la législation de protection des données à caractère personnel », *Journal des tribunaux*, 2017, p. 752.

[18] § 137 de l'arrêt *Satamedia*.

l'ensemble des traitements de données à caractère personnel qui sont couverts par les règles de protection contenues dans la Convention. Tous les domaines d'activité de l'État, des entreprises, des associations, des individus, dans lesquels il est fait recours à des traitements de données sont visés.

La Convention se distingue sur ce point des autres instruments juridiques en la matière tel le RGPD. À la différence de ce dernier, entrent ainsi dans son champ d'application les traitements de données effectués dans les domaines de la justice, de la lutte en matière pénale, de la défense, de la sécurité publique et la sûreté de l'État. Des exceptions aux dispositions susceptibles d'entraver l'efficacité de l'action dans ces domaines, ou qui conduiraient à porter atteinte à la séparation des pouvoirs, sont assurément prévues par le texte[19], mais il n'est plus question, comme par le passé[20], de permettre à une Partie de sortir du champ d'application de la Convention des catégories de traitements, tels ceux des services en charge de la sûreté de l'État.

Ce sont en outre non seulement les traitements de données à caractère personnel entièrement ou partiellement automatisés qui entrent dans le champ de la Convention mais aussi désormais les traitements ne faisant intervenir aucun procédé automatisé mais portant sur des données à caractère personnel figurant au sein « *d'un ensemble structuré de données qui sont accessibles ou peuvent être retrouvées selon des critères spécifiques* »[21]. Si la protection intervient dès qu'il y a recours à des technologies de l'information pour traiter des données à caractère personnel, elle couvre donc aussi les données reprises sur des supports papier et figurant dans un fichier ou un registre, un trombinoscope imprimé, un carnet d'adresses, une feuille de présence, un listing d'entrées, un annuaire téléphonique, etc. Le critère, dans ce cas, est que l'ensemble des données soit structuré selon un critère spécifique (ordre alphabétique, chronologique ou autre).

B. – *Critère de la juridiction*

Il a été décidé au cours des travaux de révision de la Convention de faire désormais référence à la notion de « juridiction » plutôt qu'à celle de « territoire » pour définir le champ d'application de la Convention 108+. Ainsi, alors que selon le texte de 1981, « *Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant ("protection des données")* »[22], l'article 3, § 1er de la Convention 108+ énonce : « *Chaque Partie s'engage à appliquer la présente Convention aux traitements de données relevant de sa juridiction dans les secteurs public et privé, garantissant ainsi à toute personne le droit à la protection de ses données à caractère personnel.* »[23]

[19] Voy. article 11 et article 14, § 4, c de la Convention 108+.
[20] Voy. l'article 3, § 2, a, de la Convention 108 du 28 janvier 1981.
[21] Article 2, c de la Convention 108+.
[22] Article 1er de la Convention 108.
[23] Nous soulignons.

Cette modification vise à mettre le champ d'application spatial de la Convention 108 en phase avec celui de la Convention européenne des droits de l'homme qui dispose en son article 1er que « *Les Hautes Parties contractantes reconnaissent à toute personne relevant de leur juridiction les droits et libertés définis au titre I de la présente Convention* ». La proximité entre la Convention 108 et l'article 8 CEDH attestée par la Cour européenne des droits de l'homme à maintes reprises plaide en faveur d'une mise en cohérence des champs spatiaux des deux textes.

Préférer le critère de juridiction à celui de territoire devrait aussi offrir une meilleure capacité d'adaptation du texte à une réalité mouvante qui fait de plus en plus fi d'un ancrage territorial.

On relèvera que la Convention 108 modernisée stipule expressément que « *[l]e but de la présente Convention est de protéger toute personne physique, quelle que soit sa nationalité ou sa résidence, à l'égard du traitement des données à caractère personnel* »[24]. La protection est donc offerte dès qu'un traitement de données entre dans la juridiction d'un État ou d'une organisation internationale Partie à la Convention, et ce, indépendamment de la nationalité ou du lieu de résidence des personnes physiques dont les données sont traitées.

C. – *L'exception pour les traitements de données effectués dans le cadre d'activités exclusivement personnelles ou domestiques*

La Convention 108+ ne s'applique pas au traitement de données effectué par une personne physique dans le cadre d'activités exclusivement personnelles ou domestiques[25].

Il convient de bien cerner cette exclusion du champ d'application étant donné la portée que des activités personnelles peuvent prendre aujourd'hui quand elles sont exercées, non plus dans l'intimité d'un carnet, d'un agenda ou d'un album photos sur papier, rangés dans un tiroir, mais en ayant recours aux très efficaces services en ligne permettant notamment de diffuser des données sur autrui par le biais des réseaux sociaux ou de stocker des photos dans le cloud.

Selon le Rapport explicatif de la Convention modernisée, les traitements de données visés par l'exemption sont rattachés à des activités relevant de la sphère personnelle et liées à l'exercice de la vie privée. Il faut en ce sens entendre par « *activités personnelles ou domestiques* » « *des activités étroitement et objectivement liées à la vie privée d'une personne et qui n'ont pas d'impact significatif sur la sphère personnelle d'autrui. Elles n'ont aucun aspect professionnel ou commercial et sont exclusivement liées à des activités personnelles ou domestiques comme le stockage de photos de famille ou de photos privées sur un ordinateur, la création d'une liste comportant les coordonnées d'amis ou de membres de la famille,*

[24] Article 1er de la Convention 108+.

[25] Article 3, § 2 de la Convention 108+. Le texte de cet article évoque le traitement de données effectué par « *une personne* ». Toutefois, la version anglaise de cette disposition est plus précise et permet de comprendre qu'en toute logique ce sont les seules personnes physiques qui sont visées. Selon cette version, la Convention ne s'applique pas « to data processing carried out by *an individual* in the course of purely personal or household activities » (nous soulignons).

ou la correspondance, etc. »[26] Pour qu'un partage de données puisse être considéré comme effectué au sein de la sphère privée – et dès lors se trouver en dehors du champ d'application de la Convention – il faut qu'il ait lieu par exemple au sein « *de la famille, d'un cercle restreint d'amis ou d'un cercle limité en taille, fondé sur une relation personnelle ou une relation de confiance particulière* »[27]. Le Rapport explicatif précise encore que les données « *ne peuvent pas être accessibles à un nombre indéterminé de personnes, ni même à un trop grand nombre, ni enfin à des personnes qui ne présentent pas de lien (familial, affectif ou de connaissance) avec la personne qui traite les données* »[28]. Ainsi, l'exemption ne sera pas applicable pour des données à caractère personnel rendues accessibles à un grand nombre de personnes ou à des personnes manifestement étrangères à la sphère privée, comme lors d'une diffusion sur un site web.

IV. – DÉFINITION DES PRINCIPALES NOTIONS

A. – *Notion de donnée à caractère personnel*

La notion de « *donnée à caractère personnel* » englobe « *toute information concernant une personne physique identifiée ou identifiable ([appelée la] "personne concernée")* »[29]. Il s'agit d'un concept particulièrement large puisque, loin de se limiter aux informations privées ou confidentielles, il s'applique à l'égard de n'importe quelle information pourvu que celle-ci puisse être rattachée directement ou indirectement à un individu vivant[30].

La notion couvre toute nature d'informations : confidentielles, privées, professionnelles, commerciales ou publiques. Sur ce dernier point, précisons qu'il n'est pas question de dépouiller de toute protection les données diffusées ou rendues librement accessibles sur des sites Internet ou des pages publiques de réseaux sociaux.

La notion de données à caractère personnel couvre également toute forme d'informations (écrits, photos, sons, données de localisation, données de comportement en ligne, données biométriques, *etc.*).

Elle couvre enfin tant les données qui résultent d'éléments objectifs, vérifiables et contestables, que les données subjectives contenant une évaluation ou un jugement porté sur quelqu'un.

---

[26] Paragraphe 27 du Rapport explicatif de la Convention 108+.
[27] *Ibid.*.
[28] Paragraphe 28 du Rapport explicatif de la Convention 108+.
[29] Article 2.a de la Convention 108+.
[30] Paragraphe 30 du Rapport explicatif de la Convention 108+. On sera attentif à ne pas réduire la notion de donnée à caractère personnel aux seules données identifiantes, c'est-à-dire les données permettant d'identifier l'individu. Toute information se rapportant à un individu est à considérer comme donnée à caractère personnel dès lors que cet individu est identifiable (par l'intervention éventuelle d'autres données). Ainsi les paroles prononcées par un participant à une réunion et consignées dans le procès-verbal sont des données à caractère personnel tout autant que le nom de ce participant figurant dans le PV.

L'élément important pour cerner la notion de donnée à caractère personnel est que la personne à laquelle se rapporte l'information soit identifiée ou identifiable. L'identification dont il est question doit se comprendre non comme l'établissement de l'identité civile d'un individu mais comme *l'individualisation* de cette personne, la capacité de la distinguer et la traiter différemment des autres[31]. Cette individualisation peut se faire, par exemple, en se référant au nom de la personne directement mais également à partir « *d'un numéro d'identification, d'un pseudonyme, de données biométriques ou génétiques, de données de localisation, d'une adresse IP ou d'un autre identifiant, qui renvoient à une personne donnée ou à un appareil ou un ensemble d'appareils (ordinateur, téléphone portable, appareil photo, console de jeux, etc.)* »[32].

Si l'identification du sujet des données nécessite des délais, des efforts ou des ressources déraisonnables, ce sujet ne sera plus à considérer comme étant « identifiable » et les données se rapportant à lui seront réputées anonymes. Ce qui représente des délais, efforts ou ressources déraisonnables doit s'analyser au cas par cas, « *en tenant notamment compte de l'objet du traitement et de critères objectifs tels que le coût, les bénéfices d'une telle identification, le type de responsable du traitement ou la technologie employée, etc.* »[33]. En outre, les avancées technologiques peuvent faire fluctuer ce qui doit être considéré comme « *délais, efforts ou ressources déraisonnables* ».

B. – *Notion de traitement de données*

La notion de « traitement de données » a pris la place dans la version modernisée de la Convention de celle de « fichier automatisé » utilisée dans le texte initial mais qui ne correspondait plus aux réalités technologiques actuelles.

Aux termes de l'article 2, b, de la Convention 108+, le « traitement de données » s'entend de « *toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, telles que la collecte, l'enregistrement, la conservation, la modification, l'extraction, la communication, la mise à disposition, l'effacement ou la destruction des données, ou l'application d'opérations logiques et/ou arithmétiques à ces données* ».

Les opérations entrant dans la notion de traitement de données sont donc particulièrement variées et vont de la collecte à la destruction des données. En fait, tout ce qui peut être fait avec des données à caractère personnel, tout type d'actions ou d'utilisations des données entre dans la définition de « traitement de données ».

C. – *Notions de responsable du traitement et de sous-traitant*

Les deux principales catégories d'acteurs en présence d'un traitement de données à caractère personnel sont le responsable du traitement et son éventuel sous-traitant.

[31] Paragraphe 18 du Rapport explicatif de la Convention 108+.
[32] Paragraphe 18 du Rapport explicatif de la Convention 108+.
[33] Paragraphe 17 du Rapport explicatif de la Convention 108+.

1. – *Le responsable du traitement*

Selon l'article 2, c, de la Convention, la notion de responsable du traitement signifie « *la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, dispose du pouvoir de décision à l'égard du traitement de données* ».

Ainsi, alors que cet acteur principal dans le traitement de données à caractère personnel était identifié dans la version initiale de la Convention 108 comme étant la personne compétente pour décider de la finalité du fichier automatisé, des catégories de données visées et des opérations qui leur sont appliquées, il est cette fois recouru à un critère moins détaillé mais destiné à éclairer davantage sur le rôle décisif du responsable du traitement à l'égard du traitement effectué sur les données. C'est donc la personne qui exerce le pouvoir de décision sur ce traitement. Ce pouvoir de décision peut porter sur les motifs justifiant le traitement, à savoir ses finalités, ainsi que sur les moyens utilisés pour traiter les données. On peut également tenir compte du fait de contrôler ou non les méthodes du traitement, le choix des données à traiter et les personnes autorisées à y accéder.[34]

L'identification du responsable du traitement peut découler d'une désignation officielle ou de circonstances factuelles à apprécier au cas par cas[35].

Il est encore à noter que le rôle de responsable du traitement peut être tenu par plusieurs personnes conjointement, les « *coresponsables* »[36] qui sont soit conjointement responsables d'un même traitement soit en charge de différents aspects d'un traitement[37].

2. – *Le sous-traitant*

L'insertion de la notion de sous-traitant dans la liste des définitions de la Convention 108+ répond à la nécessité d'identifier des acteurs qui jouent un rôle aujourd'hui déterminant dans les traitements de données. Aux termes de l'article 2, f, de la Convention, on vise par là « *la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* ».

Il s'agit donc de la personne, au sens large, qui travaille pour le compte du responsable du traitement, pour effectuer les tâches (généralement techniques) que ce responsable n'est pas à même d'effectuer et qu'il lui délègue. Le sous-traitant est une personne extérieure au responsable du traitement ; il ne peut s'agir d'un employé de ce dernier. Il doit accomplir les opérations de traitement conformément aux instructions du responsable du traitement. Ces instructions tracent les limites de l'utilisation autorisée des données à caractère personnel par le sous-traitant[38].

[34] Paragraphe 22 du Rapport explicatif de la Convention 108+.
[35] *Ibid.*.
[36] *Ibid.*.
[37] *Ibid.*.
[38] Paragraphe 24 du Rapport explicatif de la Convention 108+.

Cette catégorie d'acteurs joue un rôle prépondérant dans le contexte d'aujourd'hui, notamment au niveau de l'offre de services d'hébergement, de cloud, de réseaux sociaux, *etc*.. Il s'est dès lors avéré indispensable d'intégrer les sous-traitants dans le texte de la Convention afin d'encadrer leur intervention dans les traitements de données et de leur voir confier certaines responsabilités (voy. ce qui est dit ci-dessous à propos des obligations prévues à l'article 10 de la Convention). Et cela, même si la pratique a mis au jour les difficultés d'application que la notion soulevait. Il n'est en effet pas toujours évident de distinguer les notions de responsable du traitement et de sous-traitant. C'est particulièrement vrai lorsqu'on se trouve en présence d'une organisation complexe comme une entreprise multinationale ou un groupement d'entreprises ou lorsque le même acteur endosse plusieurs rôles (comme Facebook, à la fois sous-traitant pour ses utilisateurs qui choisissent de faire appel à ses services pour communiquer et partager des informations avec leurs « amis », et responsable de traitement pour l'utilisation des données que Facebook fait pour financer ses services).

V. – PRINCIPES DE BASE DE LA PROTECTION

Un ensemble de principes de base doivent être respectés pour réaliser la protection des données à caractère personnel faisant l'objet d'un traitement. Ce catalogue de principes et d'exigences est inscrit au chapitre II de la Convention 108+. Il concerne tout d'abord les conditions de légitimité des traitements des données (présentées au point A. ci-dessous) et les exigences relatives à la qualité des données (point B.) ainsi que le régime de protection accrue réservé aux données sensibles (point C.). Il poursuit avec les obligations de sécurité et de transparence qui pèsent sur le responsable de traitement et, le cas échéant, sur son sous-traitant. Une série de droits garantissent par ailleurs aux personnes concernées leur information et dès lors leur pouvoir de décision, d'action et de surveillance quant au sort réservé à leurs données. Ces obligations et ces droits sont présentés aux chapitres VI et VII ci-après.

Ces principes, obligations et droits ne sont pas absolus. Des exceptions à une partie des conditions de légitimité du traitement des données (l'exigence de loyauté, le principe de finalité et l'exigence de qualité des données), ainsi qu'à l'obligation de transparence et aux droits des personnes concernées, sont admises[39]. Elles sont décrites au chapitre VIII ci-dessous.

A. – *Conditions de la légitimité des traitements de données*

1. – *Respect du principe de proportionnalité*

La version modernisée de la Convention 108 contient une disposition particulièrement importante qui pourrait jouer un rôle crucial face au développement de traitements de données qui mettent à mal l'équilibre entre quête d'efficacité et protection des droits et libertés (dans le secteur public) ou entre intérêts économiques et protection de ces mêmes droits et libertés (dans le secteur privé). Dès lors que l'on va toujours plus loin dans le « techniquement possible » et que les

[39] Article 11, § 1er de la Convention 108+.

intérêts économiques liés à l'exploitation des données à caractère personnel sont toujours plus grands, cette disposition impose de réfléchir à l'acceptabilité des systèmes d'information et des utilisations des données envisagés.

Il s'agit de l'article 5, § 1er, de la Convention 108+ qui instaure l'obligation de respecter le principe de proportionnalité lors de la mise en œuvre des traitements de données. Ainsi, aux termes de cette disposition, « *le traitement de données doit être proportionné à la finalité légitime poursuivie et refléter à chaque étape du traitement un juste équilibre entre tous les intérêts en présence, qu'ils soient publics ou privés, ainsi que les droits et les libertés en jeu* ».

Tout traitement de données doit donc être proportionné, c'est-à-dire pertinent au regard de la finalité légitime poursuivie et limité à ce qui est nécessaire au regard des intérêts, droits et libertés des personnes concernées ou de l'intérêt public. Il ne doit pas induire une ingérence disproportionnée dans ces intérêts, droits et libertés[40].

L'article 5, § 1er, précise que le principe de proportionnalité doit être respecté à toutes les étapes du traitement, à commencer donc par le stade initial, c'est-à-dire lorsqu'il est décidé de procéder ou non au traitement des données[41], et ensuite lors de chaque opération effectuée sur les données, notamment lors de leur utilisation, de leur communication à un tiers ou de leur interconnexion avec d'autres données.

Il est donc désormais particulièrement clair qu'il faut mettre en balance l'ensemble des droits et libertés en jeu avant le lancement de tout traitement de données, et que les opérations ne peuvent être réalisées sur des données que si le résultat de la mise en balance est équilibré. Et cela, même si on a obtenu le consentement des personnes concernées. En effet, comme le Rapport explicatif le signale, « *[l]'expression d'un consentement ne dispense pas de respecter les principes fondamentaux de la protection des données à caractère personnel énoncés au chapitre II de la Convention : la proportionnalité du traitement, par exemple, doit toujours être considérée* »[42]. Ainsi, l'exigence de proportionnalité peut servir de rempart non seulement face aux risques de certains développements (comme les traitements de données insoupçonnés qui foisonnent sur Internet) mais aussi face au recours très (abusivement ?) répandu au consentement des personnes concernées pour traiter leurs données. Si la présence d'un consentement permet de présumer la légitimité d'un traitement, la mise en balance des intérêts en présence et la vérification de l'équilibre atteint offre une sauvegarde bienvenue quand on songe aux défauts trop souvent attachés au consentement (information insuffisante de la personne concernée, manifestation du consentement déduite de la non-modification de conditions par défaut, *etc*.). De plus, le consentement exprimé par la personne concernée ne reflète que la prise en compte de ses intérêts, droits et libertés propres et non de ceux d'autrui ou de la collectivité. Ce que l'un est prêt à accepter par facilité ou intérêt économique n'est peut-être pas souhaitable à l'échelle de la société dans son ensemble. On pourrait dès lors contester un tel traitement de données au nom du non-respect de l'exigence de proportionnalité.

[40] Paragraphe 40 du Rapport explicatif de la Convention 108+.
[41] *Ibid*..
[42] Paragraphe 44 du Rapport explicatif de la Convention 108+.

2. – *Nécessité d'un fondement légitime du traitement des données*

Dans sa version de 1981, la Convention était muette sur la nécessité d'un fondement légitime pour qu'un traitement de données soit admissible. La version de 2018 apporte un correctif à cette situation et introduit une disposition qui énonce les hypothèses de légitimité des traitements de données à caractère personnel. Ainsi, alors que la Convention ne réservait jusque-là aucune place au consentement de l'individu, elle stipule désormais qu'un traitement de données ne peut être effectué « *que sur la base du consentement libre, spécifique, éclairé et non-équivoque de la personne concernée ou en vertu d'autres fondements légitimes prévus par la loi* »[43].

Étant donné qu'il ne conviendrait pas pour un traité international de présenter une liste trop détaillée d'hypothèses retenues, c'est dans le Rapport explicatif qu'on trouve les éclaircissements quant aux « *autres fondements légitimes prévus par la loi* ». Celui-ci précise que les « *fondements légitimes prévus par la loi* » englobent « *notamment le traitement de données nécessaire à l'exécution d'un contrat (ou de mesures précontractuelles, à la demande de la personne concernée) auquel la personne concernée est partie ; à la protection d'intérêts vitaux de la personne concernée ou d'une autre personne ; à la mise en conformité avec une obligation légale incombant au responsable du traitement ; ainsi que le traitement de données réalisé pour des motifs d'intérêt public ou pour des intérêts légitimes prédominants du responsable du traitement ou d'un tiers* »[44].

Quant au consentement, pour être valable il doit être spécifique, libre, éclairé et non équivoque. Pour que le consentement soit considéré comme libre, aucune influence ou pression indues (de nature économique ou autre) ne peut être exercée sur la personne concernée qui doit disposer d'un véritable choix et doit pouvoir refuser ou retirer son consentement sans subir de préjudice[45]. La personne concernée doit par ailleurs avoir reçu l'information nécessaire sur l'étendue et l'implication de son consentement[46]. Cette exigence va de pair avec une obligation d'information qui pèse sur le responsable du traitement (voy. *infra*). Non équivoque, le consentement doit se manifester par le biais d'une déclaration (écrite, électronique ou orale) ou d'une action affirmative qui indique clairement l'acceptation du traitement des données en cause. En conséquence, « *le silence, l'inaction ou des formulaires ou cases à cocher prévalidés ne peuvent constituer un consentement* »[47]. En outre, le consentement couvre l'ensemble des opérations de traitement de données qui poursuivent la même finalité de sorte que « *lorsque les finalités sont multiples, un consentement doit être donné pour chacune d'entre elles* »[48].

[43] Article 5, § 2, de la Convention 108+.
[44] Paragraphe 46 du Rapport explicatif de la Convention 108+.
[45] Paragraphes 42 et 45 du Rapport explicatif de la Convention 108+.
[46] Paragraphe 42 du Rapport explicatif de la Convention 108+.
[47] *Ibid*..
[48] *Ibid*..

3. – *Loyauté et transparence du traitement des données*

L'exigence de loyauté[49] induit que le traitement des données est réalisé dans la transparence pour les personnes concernées, et sans tromperie. Les traitements de données ne peuvent se faire à l'insu des personnes sur qui portent les données. Le principe de loyauté est intimement lié au devoir de transparence. Ce devoir de transparence implique que certaines informations soient fournies spontanément par le responsable du traitement aux personnes concernées[50]. L'idée est d'annoncer loyalement aux personnes concernées le sort qui attend leurs données.

La loyauté du traitement des données ne se limite pas au moment de la collecte, mais doit être garantie à toutes les étapes de celui-ci.

C'est un problème de loyauté qui fut au cœur du scandale « Cambridge Analytica »[51] : les utilisateurs de Facebook étaient invités à répondre à un test de personnalité pour lequel ils étaient amenés à croire qu'ils opéraient dans le cadre d'une étude universitaire et que le but poursuivi était dès lors académique, alors qu'en réalité l'objectif de la récolte des données était commercial et de prospection politique[52]. C'était également un manque de loyauté qui fut reproché à Facebook – encore – du fait de sa collecte (grâce au module social « datr ») de données sur des internautes non inscrits sur ce réseau social et navigant hors de Facebook, et dès lors ne s'attendant pas un seul instant à ce que Facebook recueille des traces de leur navigation[53].

4. – *Respect du principe de finalité*

Principe fondamental de la protection des données, le principe de finalité impose que les données à caractère personnel soient « *collectées pour des finalités explicites, déterminées et légitimes et ne [soient] pas traitées de manière incompatible avec ces finalités* ».[54] En exigeant que les responsables de traitement déterminent dès le départ le but précis de leur démarche, on fournit le fil rouge qui

[49] Article 5, § 4, a) de la Convention 108+.
[50] Voir l'article 8 de la Convention 108+.
[51] C. CADWALLADR et E. GRAHAM-HARRISON, « Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach », *The Guardian*, 17 mars 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election ; CNIL, « Affaire Cambridge Analytica/Facebook », 12 avril 2018, https://www.cnil.fr/fr/affaire-cambridge-analytica-facebook.
[52] Voy. É. DEGRAVE, « Cambridge Analytica: et la vie privée ? », *Journal de Droit Européen.*, 2018, 213.
[53] Délibération de la formation restreinte de la CNIL SAN-2017-006 du 27 avril 2017 prononçant une sanction pécuniaire (de 150.000 €) à l'encontre des sociétés FACEBOOK INC. et FACEBOOK IRELAND. https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000034728338&fastReqId=390211096&fastPos=2. Également Trib. Civ. Bruxelles, 16 février 2018, n° de rôle 2016/153/A. E. DEGRAVE, « Facebook, les cookies et la justice belge : le retour », Justice en ligne, 22 mars 2018, http://www.justice-en-ligne.be/article1044.html. Les condamnations prononcées se basent sur les lois de protection des données française et belge, lois conformes à la version modernisée de la Convention 108+.
[54] Article 5, § 4, b), de la Convention 108+.

permettra de savoir quelles données peuvent être collectées et utilisées pour servir ce but, quelles actions peuvent être réalisées avec ces données, à qui elles pourront être communiquées et combien de temps elles pourront être conservées. Seules les opérations et les communications compatibles avec les finalités de départ sont admises.

Le fait que la finalité doit être explicite vient appuyer la volonté de transparence pour contrecarrer l'opacité qui règne aujourd'hui dans les traitements de données.

La référence à des « *finalités déterminées* » indique qu'il n'est pas permis de traiter des données pour des finalités non définies, imprécises ou vagues[55]. Il faut atteindre un seuil suffisant de précision de l'objectif poursuivi par la mise en œuvre d'un traitement de données. Le seul renvoi aux missions d'un service administratif, par exemple, ne répond pas à cette exigence de finalités déterminées.

Enfin, pour que la finalité du traitement de données soit légitime, il faut ménager un juste équilibre entre les droits et intérêts de la personne concernée et ceux du responsable du traitement ou de la société[56]. On n'admettra pas comme légitime un objectif qui causerait une atteinte excessive aux personnes concernées. On retrouve au niveau de la finalité, l'exigence de proportionnalité existant pour l'ensemble du traitement des données (cf. point 1. *supra*).

Le principe de finalité implique aussi que seules les utilisations compatibles avec la ou les finalités déterminées et annoncées au départ, au moment de la collecte, sont admises[57]. La notion d'utilisation « compatible » doit s'entendre en tenant compte des nécessités de transparence et de loyauté du traitement de données[58]. En particulier, les données à caractère personnel ne doivent pas faire l'objet d'un traitement ultérieur que la personne concernée pourrait considérer comme inattendu, inapproprié ou contestable[59].

Cet aspect du principe de finalité se retrouve également dans la jurisprudence de la Cour européenne des droits de l'homme. Dans l'affaire *M.S. c. Suède*[60], des données médicales confidentielles, personnelles et sensibles d'une patiente avaient été communiquées, sans le consentement de celle-ci, d'une autorité publique à une

[55] Paragraphe 48 du Rapport explicatif de la Convention 108+.
[56] *Ibid.* La jurisprudence de la Cour européenne des droits de l'homme va dans le même sens : dans son arrêt *S. et Marper*, la Cour a ainsi affirmé que le traitement de données doit être proportionné, c'est-à-dire approprié par rapport aux buts légitimes poursuivis, nécessaire dans la mesure où il n'existe pas d'autres mesures appropriées moins attentatoires aux intérêts, droits et libertés des personnes concernées ou de la société, et qu'il ne peut induire une atteinte démesurée à ces intérêts, droits et libertés par rapport aux bénéfices attendus par le responsable du traitement (Cour EDH, Grande Chambre, 4 décembre 2008, *S. et Marper c/ Royaume-Uni*, requêtes n° 30562/04 et 30566/04, § 118).
[57] Article 5, § 1er de la Convention 108 +.
[58] Rapport explicatif du protocole d'amendement à la Convention 108, précit., § 49.
[59] *Ibid.* Le Rapport explicatif énonce une série de critères permettant d'établir si l'utilisation des données à une autre fin est compatible ou non avec la finalité de la collecte de départ. Ces critères sont : le lien pouvant exister entre les deux finalités, le contexte, la nature des données, les conséquences du traitement ultérieur et des garanties existantes.
[60] Cour EDH, 27 août 1997, *M.S. c/ Suède*.

autre. Selon la Cour, « la communication ultérieure servait un but différent » et « *[…] la divulgation des informations dépendait d'une série d'éléments dont la maîtrise échappait à l'intéressée* »[61]. En conséquence, la Cour a estimé que la communication des données avait porté atteinte au droit au respect de la vie privée de la patiente. Pour que cette atteinte soit admissible, il faut que la communication des données soit prévue par une norme accessible suffisamment précise.

La Convention 108+ précise à l'article 4, § 4, b, que le traitement ultérieur des données à caractère personnel à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques est *a priori* jugé compatible à deux conditions :

- « *que des garanties complémentaires s'appliquent* ». À titre d'exemples de garanties complémentaires, le Rapport explicatif cite « *l'anonymisation ou la pseudonymisation des données sauf s'il est indispensable de conserver la forme identifiable, des règles en matière de secret professionnel, des dispositions régissant l'accès restreint et la diffusion restreinte de données aux fins précitées, notamment celles liées aux statistiques et à l'archivage public, ainsi que d'autres mesures d'ordre technique et organisationnel visant la sécurité des données* »[62] ; et

- que les opérations de traitement des données « *excluent, en principe, toute utilisation de l'information obtenue pour la prise de décisions ou de mesures concernant une personne donnée* »[63]. Les finalités archivistiques, statistiques et de recherche scientifique ne peuvent, en principe[64], déboucher sur une prise de décision ou une mesure individuelle.

Enfin on relèvera que du principe de finalité découle l'exigence de ne pas conserver les données plus longtemps que nécessaire pour atteindre la ou les finalités[65].

B. – *Exigences relatives à la qualité des données*

Déjà présentes dans la version de 1981 de la Convention, les exigences liées à la qualité des données ont traversé le temps sans prendre une ride et sont toujours d'actualité dans la version de 2018. Les données à caractère personnel doivent donc toujours bien être « *adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont traitées* » [66] ainsi qu'« *exactes et si nécessaire mises à jour* »[67].

[61] *Ibid.*, § 35.
[62] Paragraphe 50 du Rapport explicatif de la Convention 108+.
[63] *Ibid*.
[64] Il peut arriver, dans le cadre par exemple d'une recherche médicale sur la base de données codées, que l'on décide, au vu des résultats de la recherche, de remonter jusqu'aux patients pour modifier leur traitement, et prendre donc une mesure individuelle.
[65] Article 5, § 4, e de la Convention 108+.
[66] Article 5, § 4, c de la Convention 108+.
[67] Article 5, § 4, d de la Convention 108+.

Pour être jugées adéquates et pertinentes, les données doivent présenter un lien nécessaire et suffisant avec les finalités poursuivies[68]. Il est fréquent, en réalité, qu'on soit confronté à des récoltes d'informations qui dépassent ce qui est pertinent au vu du but poursuivi : formulaire de commande d'un bien demandant la date de naissance, collecte du numéro national pour l'octroi d'une carte de fidélité, caméra de surveillance à l'entrée d'une maison débordant sur le voisinage…

L'exigence de données non excessives, quant à elle, est une invitation explicite à la modération. Cette disposition vise aussi bien les aspects quantitatifs que qualitatifs des données à caractère personnel faisant l'objet d'un traitement[69]. Cela signifie d'une part qu'il faut veiller à ne pas récolter plus de données que nécessaire et, d'autre part, que, même pertinentes, les données qui induisent une atteinte excessive à la personne concernée ne doivent pas être traitées. C'est le cas notamment de la communication à l'employeur d'un avis du médecin du travail qui révélerait en détail l'état de santé d'un travailleur. Quoique pertinentes pour permettre à l'employeur de vérifier l'aptitude au travail de la personne concernée, ces données médicales sont excessives. On ne doit admettre que la communication d'un constat d'aptitude ou d'inaptitude sans développements détaillés. D'un côté pratique, l'observation de cette exigence de minimisation peut être facilitée par le recours à des techniques d'anonymisation ou de pseudonymisation systématique ou par un paramétrage par défaut peu gourmand en données.

C. – *Régime plus protecteur pour les données sensibles*

L'identification d'une catégorie particulière de données à caractère personnel auxquelles on réserve une protection plus élevée est liée aux risques accrus de porter préjudice aux individus sur la base du traitement de ces données. C'est principalement le risque de discriminations illégitimes ou arbitraires lié à ces données qui justifie le traitement différencié qui leur est accordé. De telles données présentent, en outre, un risque d'affecter la sphère la plus intime des sujets de données ainsi qu'un risque sérieux de dommage, en cas d'abus, pour la personne concernée.

La liste des données sensibles figure à l'article 6, § 1er de la Convention 108+. On distingue :

- les données sensibles par nature, présentant en toutes circonstances un caractère sensible : il s'agit des données génétiques et des données à caractère personnel concernant des infractions pénales (y compris présumées), des procédures et des condamnations pénales et des mesures de sûreté connexes ;

- les données biométriques lorsqu'elles sont traitées aux fins d'identifier une personne physique de manière unique ;

- les données sensibles par l'usage qui en est fait : les données à caractère personnel pour les informations qu'elles révèlent sur l'origine raciale ou ethnique, les

[68] M/-H. BOULANGER, C. DE TERWANGNE, T. LÉONARD, S. LOUVEAUX, D. MOREAU, Y. POULLET, « La protection des données à caractère personnel en droit communautaire », *J.T. dr. eur.*, 1997, p. 146.
[69] Paragraphe 52 du Rapport explicatif de la Convention 108+.

opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres convictions, la santé ou la vie sexuelle[70] [71].

Les données de la dernière catégorie ne doivent être considérées comme sensibles que dans les cas où c'est précisément l'élément informationnel sensible contenu dans la donnée qui est traité. Ainsi, lorsque le traitement d'images enregistrées vise à révéler des informations sur l'origine raciale ou ethnique, ou sur la santé des personnes filmées, il s'agit d'un traitement de données sensibles. Alors qu'il s'agira d'un traitement de données ordinaires si les individus sont seulement filmés dans un contexte de vidéosurveillance à des fins de sécurité, sans chercher à traiter l'élément sensible figurant sur les images[72].

Un régime plus protecteur que pour les données ordinaires est réservé aux données sensibles, étant donné le risque plus élevé que leur traitement engendre pour la personne concernée. Leur traitement n'est autorisé qu'à la condition que des garanties appropriées, venant compléter celles de la Convention, soient prévues par la loi[73]. Deux éclaircissements sont apportés quant aux garanties qui doivent accompagner le traitement de ces données. Tout d'abord, ainsi qu'il vient d'être dit, les garanties appropriées doivent venir en supplément des mesures de protection mises en place par la Convention. On ne peut donc se contenter de renvoyer à des mesures relevant du régime général pour rendre admissible le traitement de données sensibles. Il peut s'agir de garanties juridiques ou d'une autre nature. Ensuite, les garanties appropriées sont présentées comme celles de nature à prévenir le risque grave que le traitement des données sensibles fait peser sur les intérêts,

[70] Les données génétiques et biométriques sont nouvelles dans la liste des données sensibles par rapport à la liste de 1981. Les données relatives aux condamnations pénales ont été élargies aux infractions, procédures et mesures de sûreté. Quant aux autres données, elles figuraient déjà dans la liste initiale sauf les données révélant l'appartenance syndicale. Toutefois, le Rapport explicatif de la Convention signalait que cette liste ne devait pas être considérée comme exhaustive et que les États Parties pouvaient ajouter d'autres catégories de données si le contexte sociologique l'imposait. L'exemple donné était précisément celui des informations sur l'appartenance syndicale. Il était relevé que dans certains pays ces informations étaient considérées comme entraînant des risques pour la vie privée alors que dans d'autres pays elles n'étaient considérées comme sensibles que dans la mesure où elles étaient étroitement liées aux opinions politiques. Certaines Parties les avaient donc déjà ajoutées à la liste des données sensibles.

[71] La Cour européenne des droits de l'homme a elle aussi insisté sur le caractère sensible de plusieurs types de données, telles les données médicales (Cour EDH, 25 février 1997, *Z. c/ Finlande)*, les données génétiques et biométriques. Elle a estimé que « *la conservation d'empreintes digitales constitue une atteinte au droit au respect de la vie privée* » (Cour EDH, 4 décembre 2008, *S. et Marper*, précit.) qui ne peut donc être admise que moyennant le respect des conditions du paragraphe 2 de l'article 8 CEDH. Selon la Cour, « *le droit interne doit aussi contenir des garanties aptes à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs. Les considérations qui précèdent valent tout spécialement lorsqu'est en jeu la protection de catégories particulières de données plus sensibles, notamment des données ADN, qui, dans la mesure où elles contiennent le patrimoine génétique de la personne, revêtent une grande importance tant pour elle-même que pour sa famille* » (*Ibid*., § 103).

[72] Paragraphe 59 du Rapport explicatif de la Convention 108+.

[73] Article 6, § 2 de la Convention 108+.

droits et libertés fondamentales de la personne concernée, notamment le risque de discrimination.

VI. – OBLIGATIONS DE SÉCURITÉ ET DE TRANSPARENCE

A. – *Obligation de sécurité*

1. – *Mesures de sécurité appropriées*

Il convient de protéger les données à caractère personnel contre une curiosité malsaine venant de l'intérieur ou de l'extérieur ou contre des manipulations non autorisées, qu'elles soient de nature accidentelle ou qu'elles soient malintentionnées. Un devoir d'adopter des mesures de sécurité existait déjà dans le texte initial de la Convention. Il a été repris dans la version modernisée de 2018 avec, au passage, une clarification de la responsabilité de la sécurité : elle revient au responsable du traitement ainsi qu'à son sous-traitant dans les cas où il est recouru aux services d'un sous-traitant.

Ces acteurs doivent, selon les termes de l'article 7, § 1er, de la Convention 108+, « *prend[re] des mesures de sécurité appropriées contre les risques tels que l'accès accidentel ou non autorisé aux données à caractère personnel, leur destruction, perte, utilisation, modification ou divulgation* ».

Les mesures de sécurité à prendre sont de deux ordres[74] : des mesures organisationnelles (limiter le nombre de personnes ayant accès aux données, utiliser des mots de passe renouvelés régulièrement, fermer les locaux où sont localisés les ordinateurs, *etc*.) et des mesures techniques (programme antivirus fréquemment mis à jour, *firewalls, backup* de sécurité, *login*…). Si le texte se contente de dire qu'il doit s'agir de mesures de sécurité « *appropriées* », le Rapport explicatif spécifie que le choix des mesures de sécurité doit tenir compte « *des éventuels effets dommageables pour l'individu, de la nature des données à caractère personnel, du volume de données à caractère personnel traitées, du degré de vulnérabilité de l'architecture technique utilisée pour la réalisation du traitement, de la nécessité de restreindre l'accès aux données, des impératifs d'une conservation à long terme,* etc. »[75]. L'exigence de sécurité est donc modalisable en fonction des risques que le traitement fait courir aux personnes concernées. Ainsi, plus les données en cause sont sensibles et les risques pour la personne concernée sont grands, plus importantes seront les précautions à prendre. Par exemple, des données relatives à la santé d'une personne, utilisées en dehors d'un contexte médical (par exemple, par une compagnie d'assurances pour octroyer une assurance vie), devront être encadrées de mesures de sécurité sévères.

On signale que la jurisprudence a déjà apporté un éclaircissement intéressant sur la portée de cette exigence. Il en découle que les mesures de sécurité doivent non seulement empêcher les accès non autorisés mais également permettre aux personnes concernées de contrôler les accès aux données qui ont eu lieu. Seul cet accès aux données sur les personnes ayant accédé aux données permet en effet à la personne concernée de vérifier l'effectivité des mesures de sécurité et lui permet

[74] Paragraphe 62 du Rapport explicatif de la Convention 108+.
[75] *Ibid*..

d'exercer son contrôle ou sa maîtrise sur ses propres informations. C'est en ce sens qu'a jugé la Cour européenne des droits de l'homme dans l'affaire de 2008 *I c. Finlande*, condamnant cet État pour avoir laissé un hôpital public mettre en place un système de sécurité des données qui ne conserve en mémoire que les traces des cinq derniers accès aux données et qui, de surcroît efface toute trace d'accès une fois les données versées aux archives[76].

2. – *Les violations de sécurité*

Un paragraphe supplémentaire a été ajouté à l'article 7 de la Convention 108+ sur la sécurité des données. Il concerne l'obligation de signaler la survenance d'atteintes à la sécurité d'un certain niveau de gravité. Cette nouvelle règle s'énonce de la sorte :

« *2. Chaque Partie prévoit que le responsable du traitement est tenu de notifier, sans délai excessif, à tout le moins à l'autorité de contrôle compétente au sens de l'article 15 de la présente Convention, les violations des données susceptibles de porter gravement atteinte aux droits et libertés fondamentales des personnes concernées.* »[77]

Il s'agit d'aviser l'autorité de contrôle de toute violation des données susceptible de porter gravement atteinte aux droits et libertés fondamentaux de la personne concernée. À titre d'exemples d'atteinte « grave » aux droits et libertés fondamentales des personnes concernées, le Rapport explicatif cite la révélation de données couvertes par le secret professionnel, ou de données susceptibles d'entraîner un préjudice financier (comme les données liées à une carte de crédit) ou de causer une atteinte à la réputation, des dommages corporels ou une humiliation[78].

Il y a violation de données lorsqu'un tiers non autorisé, un pirate par exemple, a accédé à des données à caractère personnel en s'introduisant illégalement dans un serveur. Entrent également dans le champ de cette notion des situations dans lesquelles les données à caractère personnel ont été perdues (par exemple, sur des CD-Rom, des clés USB ou d'autres appareils portatifs), ou communiquées par inadvertance ou malveillance par un utilisateur autorisé, en violation du principe de finalité ou de son devoir de confidentialité (par exemple, pour reprendre des cas réellement survenus : un fichier de données bancaires transmis aux autorités fiscales d'un pays tiers par un employé licencié, à titre de vengeance ; la publication accidentelle sur un site internet de la liste des personnes affiliées à un parti politique ; l'envoi par une société pharmaceutique d'un mail d'alerte à propos d'un médicament, laissant apparaître le nom et les coordonnées de toutes les personnes consommant ce médicament…). Si les conséquences de ces violations de données pour les personnes concernées peuvent être qualifiées de graves, il y a obligation de notification du problème.

[76] Cour eur. D.H., *I. v. Finlande*, 17 July 2008, appl. n° 20511/03, § 41.
[77] Article 7, § 2 de la Convention 108+.
[78] Paragraphe 64 du Rapport explicatif de la Convention 108+.

Selon le Rapport explicatif, signaler les violations de données aux autorités de contrôle est l'exigence minimale. Il faudrait également que le responsable du traitement soit tenu d'informer les autorités de contrôle des mesures prises ou envisagées pour remédier à la violation et pallier les conséquences potentielles.[79] En outre, il peut être nécessaire d'informer les personnes concernées elles-mêmes, notamment lorsque la violation des données est de nature à engendrer un risque important pour leurs droits et libertés, « *par exemple un traitement discriminatoire, un vol ou une usurpation d'identité, des pertes financières, une atteinte à la réputation, une perte de confidentialité des données protégées par le secret professionnel ou tout autre préjudice économique ou social lourd* »[80]. Il conviendrait dans ce cas de renseigner les sujets des données sur les mesures à prendre pour atténuer les effets néfastes de la violation de leurs données[81].

On relèvera enfin que cette obligation de notification des violations de données s'impose sous réserve de l'exception prévue à l'article 11, § 1er de la Convention, c'est-à-dire l'exception au nom d'intérêts publics ou privés supérieurs qui souffriraient d'une telle transparence des failles survenues dans la sécurité des données[82].

B. – *La transparence*

Un système de protection des données qui se veut crédible aujourd'hui ne peut plus s'accommoder, comme en 1981, de garanties qui reposent essentiellement sur la seule initiative de la personne concernée. Il s'est avéré impératif, vu l'environnement particulièrement opaque des systèmes d'information actuels, de mettre à charge des responsables de traitement des obligations de transparence active. La personne concernée ne peut s'intéresser à et s'informer sur un traitement dont elle ne soupçonne pas l'existence. Combien de personnes concernées « standard » songeront que les mots introduits dans un moteur de recherche sont enregistrés pendant des mois et reliés à leur identifiant ? Ou que des caméras les filment alors qu'elles sont miniaturisées et, vu leur puissance, posées à bonne distance ? Ou que le portique qu'elles franchissent lit la puce RFID qui se trouve dans leur passeport ? Les exemples de telles situations où les personnes concernées ne se doutent pas, tant qu'on ne les en a pas informées, que leurs données sont traitées, sont multipliables à l'envi aujourd'hui.

Il a donc été rapidement décidé lors du travail de modernisation de la Convention d'introduire de façon expresse une obligation d'information des personnes sur lesquelles on traite des données, à mettre à charge du responsable du traitement. Le but de cette obligation d'information est clairement « *de faire preuve de transparence dans la conduite des opérations de traitement afin de garantir un traitement loyal* »[83] et de permettre aux personnes concernées de comprendre ce qu'il se passe avec leurs données et, en conséquence, d'être capables d'exercer pleinement leurs droits dans le cadre du traitement considéré.

---

[79] Paragraphe 65 du Rapport explicatif de la Convention 108+.
[80] Paragraphe 66 du Rapport explicatif de la Convention 108+.
[81] *Ibid.*.
[82] Voir ce qui est dit *supra* à ce propos, en entame du chapitre V.
[83] Paragraphe 67 du Rapport explicatif de la Convention 108+.

Cette obligation est énoncée à l'article 8, § 1er, sous la forme suivante :

« *Chaque Partie prévoit que le responsable du traitement informe les personnes concernées :*

« *a. de son identité et de sa résidence ou lieu d'établissement habituels ;*

« *b. de la base légale et des finalités du traitement envisagé ;*

« *c. des catégories des données à caractère personnel traitées ;*

« *d. le cas échéant, des destinataires ou catégories de destinataires des données à caractère personnel ; et*

« *e. des moyens d'exercer les droits énoncés à l'article 9 ;*

« *ainsi que de toute autre information complémentaire nécessaire pour garantir un traitement loyal et transparent des données à caractère personnel.* »

Une série de renseignements doivent donc être communiqués spontanément aux personnes sur qui on traite des données – sous réserve de la possibilité pour les Parties de prévoir des exceptions conformément à l'article 11, § 1[84] et si les personnes concernées ne disposent pas déjà de ces informations[85] –: le nom et l'adresse du responsable du traitement (ou des coresponsables), la base légale et les finalités du traitement, les catégories de données traitées et leurs destinataires ainsi que les moyens d'exercer les droits. Ces informations, qui doivent être facilement accessibles et compréhensibles, peuvent être fournies sous tout format approprié (par le biais d'un site web, d'outils technologiques sur des appareils personnels, etc.) pourvu qu'elles soient présentées de manière effective et loyale à la personne concernée.[86] Parmi les « *autre[s] information[s] nécessaire[s] pour garantir un traitement loyal et licite des données* », figure notamment la durée de conservation des données ou l'information sur les pays tiers vers lesquels les données seront communiquées si elles sont effectivement destinées à partir vers l'étranger.

Deux exceptions particulières à ce devoir d'information sont prévues en plus des possibilités d'exceptions ouvertes à l'article 11 de la Convention[87]. Ces exceptions particulières n'entrent en effet pas dans les justifications d'exception admises à l'article 11, § 1er, qui sont, elles, fondées sur la sauvegarde d'intérêts publics ou privés prépondérants. Ces deux exceptions spécifiques n'interviennent que dans le cas d'une collecte indirecte des données à caractère personnel, n'impliquant donc aucun contact direct avec les personnes concernées.

L'une de ces exceptions tient compte de contraintes matérielles : le responsable du traitement n'est pas tenu de fournir les informations lorsque cela lui est impossible ou implique des efforts disproportionnés, parce que, précise le Rapport explicatif[88], la personne concernée n'est pas directement identifiable ou qu'il n'a aucun moyen de la contacter. Cette impossibilité peut être d'ordre pratique (par exemple

[84] Voir *infra* IX.
[85] Article 8, § 2 de la Convention 108+.
[86] Paragraphe 68 du Rapport explicatif de la Convention 108+.
[87] Article 8, § 3 de la Convention 108+.
[88] Paragraphe 68 du Rapport explicatif de la Convention 108+.

lorsqu'un responsable du traitement ne traite que des images et ignore le nom et les coordonnées des personnes concernées) mais peut aussi être d'ordre juridique (dans le cadre d'une enquête pénale par exemple)[89].

La seconde exception est accordée pour les traitements prévus par la loi. L'adage « *nul n'est censé ignorer la loi* » permet de considérer que les citoyens sont déjà informés mais cela n'est valable qu'à la condition que la loi en question soit suffisamment précise et apporte les renseignements nécessaires pour assurer une information loyale des personnes concernées.

VII. – DROITS DES PERSONNES CONCERNÉES

Toute personne, quels que soient son âge, son domicile ou sa nationalité, se voit reconnaître des droits vis-à-vis de ceux qui traitent des données sur elle. La Convention 108+ a étoffé remarquablement la liste des droits garantis et a renforcé les droits qui existaient déjà auparavant.

Les droits octroyés à la personne concernée visent notamment à assurer la transparence sur demande des traitements de données. Cette transparence doit permettre à la personne concernée non seulement d'avoir connaissance, mais aussi de contrôler ce qui est fait avec ses données, de vérifier le respect des règles, de traquer les abus ou les illégalités, de s'opposer, de corriger les erreurs. Cela étant, le premier droit consacré dans la liste est, quant à lui, lié à la dignité humaine, il s'agit du droit de ne pas être soumis à une décision automatisée.

Avant de passer ces droits en revue, il y a lieu de rappeler qu'ils ne sont pas absolus et que des exceptions sont admises moyennant les conditions indiquées à l'article 11 de la Convention 108+. Ainsi, les exceptions doivent être prévues par la loi, respecter l'essence des droits et libertés fondamentales et être nécessaires, dans une société démocratique, à la protection des intérêts supérieurs publics ou privés listés à l'article 11, § 1, a et b.[90]

A. – *Le droit de ne pas être soumis à une décision individuelle automatisée*

Il a paru impératif pour les auteurs de la modernisation de la Convention 108 de consacrer en premier lieu le droit pour toute personne de « *ne pas être soumise à une décision l'affectant de manière significative, qui serait prise uniquement sur le fondement d'un traitement automatisé de données, sans que son point de vue soit pris en compte* »[91].

Présenté comme premier droit de la personne concernée, ce droit découle de la volonté farouche que l'homme ne soit pas soumis entièrement à la machine. Il n'est pas souhaitable qu'une décision qui s'impose à un individu dépende des seules

[89] *Ibid.*.
[90] Voir les développements au paragraphe 91 du Rapport explicatif de la Convention 108+. Voir égal. *infra* IX.
[91] Article 9, § 1, a, de la Convention 108+.

conclusions d'une machine. C'est là l'expression de la prééminence à accorder à la dignité humaine[92].

Or, la technique est de plus en plus souvent utilisée aujourd'hui pour s'en remettre à un « ordinateur » et aux algorithmes qu'il applique pour décider du sort à réserver à un individu (le considérer ou non comme fraudeur fiscal, comme cible de marketing ou comme voyageur candidat terroriste, …). Au nom de la dignité humaine, il est crucial que l'individu puisse faire valoir de manière effective son point de vue et ses arguments et puisse, par-là, contester la décision. « *En particulier, la personne concernée doit avoir la possibilité de prouver l'inexactitude éventuelle des données à caractère personnel avant leur utilisation, l'inadéquation du profil qu'il est prévu d'appliquer à sa situation particulière ou d'autres facteurs qui auront un impact sur le résultat de la décision automatisée.* »[93]

Toutefois, l'interdiction de soumettre un individu à une décision entièrement automatisée ne s'applique pas lorsque la décision est autorisée par une loi à laquelle est soumis le responsable du traitement[94]. Pour que la décision automatisée soit admissible, cette disposition légale doit prévoir des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée[95].

B. – *Le droit d'accès*

Depuis quarante ans les individus se voient garantir le droit d'avoir connaissance de l'existence des traitements de données à leur propos et de la teneur des informations faisant l'objet d'un traitement.

Il a été décidé lors du processus de modernisation de la Convention d'enrichir ce droit d'accès[96] et d'y intégrer le droit d'accéder sur demande à toutes les informations que le responsable est en principe tenu de communiquer spontanément aux personnes concernées[97]. Des exceptions pouvant exister à ce devoir de transparence spontanée, il se peut qu'un individu n'ait reçu aucune information particulière sur le traitement effectué avec ses données et souhaite connaître par exemple l'identité du responsable du traitement ainsi que ses coordonnées, ou les finalités du traitement, ou encore les destinataires des données. Il peut donc prendre l'initiative de réclamer ces informations.

Par ailleurs, le droit d'accès a aussi été enrichi pour couvrir l'accès à l'origine des données. Cette information est en effet cruciale car c'est souvent la source des données qui intrigue et interpelle les personnes concernées (comment ont-ils obtenu ces informations ? Qui les leur a communiquées ?). D'autre part, les renseignements sur l'origine des données permettent de vérifier la licéité de la communication ou de la collecte de celles-ci et éventuellement d'introduire un recours à l'encontre du premier détenteur des données (ce qui permet « d'arrêter

[92] Cf. *supra* ce qui est dit à propos de la dignité humaine.
[93] Paragraphe 75 du Rapport explicatif de la Convention 108+.
[94] Article 9, § 2, de la Convention 108+.
[95] Paragraphe 75 du Rapport explicatif de la Convention 108+.
[96] Article 9, § 1, b, de la Convention 108+.
[97] Voir *supra*.

l'hémorragie » si celui-ci diffuse illicitement les données en question). Enfin, en cas de problèmes liés à la qualité des données et de nécessité de correction, il devient possible de faire effectuer ces corrections à la source, ce qui évite la propagation ultérieure d'erreurs.

Dans la nouvelle formulation qui est proposée, le droit d'accès s'entend donc du droit pour chaque personne concernée d' « *d'obtenir, à sa demande, à intervalle raisonnable et sans délai ou frais excessifs, la confirmation d'un traitement de données la concernant, la communication sous une forme intelligible des données traitées, et toute information disponible sur leur origine, sur la durée de leur conservation ainsi que toute autre information que le responsable du traitement est tenu de fournir au titre de la transparence des traitements conformément à l'article 8, paragraphe 1* »[98].

C. – *Le droit à connaître le raisonnement qui sous-tend le traitement des données*

Toute personne a le droit d'obtenir, à sa demande, connaissance du raisonnement qui sous-tend le traitement de données, lorsque les résultats de ce traitement lui sont appliqués[99] y compris les conséquences de ce raisonnement et les conclusions qui peuvent en avoir été tirées, en particulier lors de l'utilisation d'algorithmes pour une prise de décision automatisée, notamment dans le cadre du profilage[100].

Ce droit présente un grand intérêt face au déploiement exponentiel du phénomène de profilage. Ce phénomène est particulièrement répandu sur Internet où il est utilisé dans le cadre du cybermarketing ou d'autres domaines d'activité pour analyser ou prédire des aspects de la vie de la personne concernée. Mais il indique dépasser les limites du profilage, même si un tel droit s'impose spécialement face au phénomène où l'on s'appuie sur des « *profils* »[101] pour prendre des décisions au sujet d'une personne ou prévoir ses préférences, ses comportements et ses attitudes personnels[102]. Il est clair que même en dehors de l'hypothèse du profilage, on peut souhaiter comprendre ce qui se passe en accédant au raisonnement sous-tendant le traitement des données. Face au refus d'un crédit, aux résultats d'un examen, à la non-sélection d'une offre faite en réponse à un appel d'offres, *etc*., on peut légitimement souhaiter connaître les critères qui ont joué et le poids accordé à chacun d'eux pour évaluer la capacité de remboursement, corriger et évaluer l'examen ou apprécier la qualité de l'offre.

---

[98] Article 9, § 1, b, de la Convention 108+.
[99] Article 9, § 1, c, de la Convention 108+.
[100] Paragraphe 77 du Rapport explicatif de la Convention 108+.
[101] Le profil désigne « *un ensemble de données qui caractérise une catégorie d'individus et qui est destiné à être appliqué à un individu* » (point 1.d. de l'Annexe à la Recommandation CM/Rec (2010)13).
[102] Voir la définition du « profilage » proposée par la Recommandation : « *Le "profilage" est une technique de traitement automatisé des données qui consiste à appliquer un "profil" à une personne physique, notamment afin de prendre des décisions à son sujet ou d'analyser ou de prévoir ses préférences, comportements et attitudes personnels*. ». (point 1.e. de l'Annexe à la Recommandation CM/Rec (2010)13).

Ce droit à connaître le raisonnement qui sous-tend le traitement des données est précieux en ce qu'il contribue à l'autodétermination informationnelle des individus étant donné qu'il permet à ceux-ci non seulement de savoir ce qui est fait avec leurs données mais aussi de le comprendre et éventuellement de le contester.

Il est à noter que ce droit peut être limité par les Parties à la Convention dans le respect des conditions édictées à l'article 11 de la Convention pour toute restriction. Ce sera notamment le cas où cela est nécessaire dans une société démocratique pour garantir des « *secrets protégés par la loi* », comme des secrets commerciaux.

D. – *Le droit d'opposition*

Il a été décidé d'inscrire le droit d'opposition au tableau des droits subjectifs destinés à permettre aux individus d'exercer une maîtrise sur le sort réservé à leurs données. Toute personne dispose désormais du droit « *de s'opposer à tout moment, pour des raisons tenant à sa situation, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement, à moins que le responsable du traitement ne démontre des motifs légitimes justifiant le traitement qui prévalent sur les intérêts, ou les droits et libertés fondamentales de la personne concernée* »[103].

Ce droit se justifie particulièrement lorsque le traitement des données ne repose pas sur le consentement des personnes concernées. Celles-ci, qui n'ont pu exprimer leur point de vue à l'entame du traitement, retrouvent par le biais de ce droit la possibilité de faire valoir leurs arguments auprès du responsable du traitement pour le convaincre de renoncer à traiter leurs données. Ce droit est particulièrement important dans les hypothèses où le responsable a effectué lui-même, *a priori*, la mise en balance des intérêts en présence et a estimé que le résultat était équilibré et qu'il pouvait légitimement traiter les données. Grâce au droit d'opposition, la personne concernée retrouve l'occasion de contester le résultat de la mise en balance, à tout le moins dans son cas.

La personne concernée doit faire valoir des « *raisons tenant à sa situation* » qui l'amène à s'opposer au traitement de ses données. Il incombe au responsable du traitement qui souhaite quand même poursuivre le traitement des données en question d'avancer des motifs légitimes prépondérants et de prouver donc par-là que son intérêt légitime prévaut sur les droits et intérêts de la personne concernée. Selon le Rapport explicatif, l'exercice ou la défense d'un droit en justice ainsi que des motifs de sécurité publique peuvent être considérés comme des motifs légitimes impérieux justifiant la poursuite du traitement des données contestées[104].

Il est clair que dans le contexte actuel où les traitements de données à l'insu des personnes concernées se développent à foison, il est important de rééquilibrer la situation des intervenants en garantissant un droit aux personnes concernées de se manifester et de refuser les utilisations de leurs données quand elles viennent à en prendre connaissance. Il se peut aussi que les personnes aient bien été informées des traitements envisagés mais n'ont pris la pleine mesure du sort réservé à leurs

[103] Article 9, § 1, d, de la Convention 108+.
[104] Paragraphe 78 du Rapport explicatif de la Convention 108+.

données ou des implications que ces traitements pouvaient avoir sur d'autres intérêts qu'après un certain temps. Dans de tels cas également, le droit d'opposition offre une solution opportune.

En présence d'un traitement de données à des fins commerciales, l'opposition à un tel traitement devrait entraîner de façon inconditionnelle, sans qu'il soit donc nécessaire pour la personne concernée de faire valoir des raisons tenant à sa situation, la suppression des données à caractère personnel faisant l'objet de l'opposition[105].

E. – *Le droit de rectification et d'effacement*

Le droit de rectification et d'effacement est accordé depuis l'origine de la Convention 108 aux personnes concernées. Toute personne se voit donc toujours reconnaître le droit d'« *obtenir à sa demande, sans frais et sans délai excessifs, la rectification de ces données [les données à caractère personnel la concernant] ou, le cas échéant, leur effacement lorsqu'elles sont ou ont été traitées en violation des dispositions de la présente Convention* »[106].

La précision que la rectification ou l'effacement des données doit s'obtenir « *sans frais et sans délai excessifs* » est une nouveauté bienvenue introduite dans la version modernisée de la Convention. On signalera qu'une erreur s'est glissée dans la version française de la Convention 108+ qui présente le mot « *excessif* » au pluriel alors qu'il ne se rapporte qu'au « délai » et non aux « frais ». La version anglaise du texte est très éclairante puisqu'elle stipule que la rectification ou l'effacement des données doit s'obtenir « free of charge and without excessive delay ». Le droit de rectification doit donc pouvoir s'exercer gratuitement (si une donnée est incorrecte ou si son traitement est illicite, on ne comprendrait pas qu'il faille payer pour faire rectifier une erreur ou pour faire cesser une illicéité…). La correction ou l'effacement doivent par ailleurs intervenir sans délai excessif, notion qui permet d'adapter aux situations l'exigence de rapidité de la réaction. Ainsi, on ne tolérera pas que la correction d'une erreur flagrante relative à une information diffusée sur Internet prenne une semaine alors qu'on accordera plus de temps pour la contestation d'une donnée d'un service administratif qui nécessite des vérifications.

Les rectifications et effacements obtenus à la suite de l'exercice de ce droit, « *doivent, dans la mesure du possible, être portés à la connaissance des destinataires de l'information originale, à moins que cela se révèle impossible ou implique des efforts disproportionnés* »[107].

On notera enfin qu'il a été décidé lors des travaux de modernisation de la Convention de ne pas proposer l'introduction explicite d'un « droit à l'oubli » dans le texte révisé de la Convention. Il a en effet été considéré que la conjugaison des garanties existantes peut offrir une protection efficace aux personnes concernées sans porter atteinte au droit à la liberté d'expression. Ainsi, le droit de rectification

[105] Paragraphe 79 du Rapport explicatif de la Convention 108+.
[106] Article 9, § 1, e, de la Convention 108+.
[107] Paragraphe 81 du Rapport explicatif de la Convention 108+.

et d'effacement des données incorrectes, incomplètes ou injustifiées, associé à un droit effectif d'opposition au traitement, apporte une forme de réponse à la préoccupation liée au droit à l'oubli. Par ailleurs, la règle dérivant du principe de finalité, imposant une durée de conservation des données réduite en fonction de la finalité du traitement à atteindre, conduit à l'effacement des données dès que celles-ci ne présentent plus d'utilité pour réaliser l'objectif du traitement.

F. – *Le droit de recours*

Aux termes de l'article 9, § 1, f, de la Convention, un recours doit être mis à la disposition de toute personne qui voit ses droits bafoués, à qui par exemple le responsable du traitement n'a pas répondu ou les cas où celui-ci n'a pas corrigé ou effacé les données malgré une demande en ce sens ou n'a pas cessé le traitement des données alors que la personne concernée s'y était opposée.

Cette disposition doit être lue en combinaison avec l'article 12 qui porte sur les « Sanctions et recours ». Il y est prévu que chaque Partie s'engage à établir des recours juridictionnels et non juridictionnels appropriés visant les violations du droit interne donnant effet aux dispositions de la Convention. La nature des recours mis en place (civils, administratifs, pénaux) est laissée à la discrétion de chaque État ou organisation internationale Partie.

On a pu constater que « *[l] a plupart des pays disposant d'une loi en matière de protection des données ont institué à cet égard une autorité de contrôle, généralement un commissaire, une commission, un ombudsman ou un inspecteur général. Ces autorités de contrôle dans le domaine de la protection des données fournissent un recours approprié lorsqu'elles sont dotées de compétences effectives et qu'elles jouissent d'une réelle indépendance dans l'exercice de leurs fonctions. Elles sont devenues partie intégrante du système de contrôle de la protection des données dans une société démocratique* »[108]. Pour être reconnues comme une voie de recours appropriée contre les violations des règles de protection des données, ces autorités de contrôle doivent se voir confier le pouvoir de trancher les litiges, ainsi que des pouvoirs d'intervention et d'injonction[109].

G. – *Le droit à l'assistance d'une autorité de contrôle*

Ainsi qu'il vient d'être dit, les individus peuvent se tourner vers les autorités de contrôle nationales pour exercer leur droit de recours contre le non-respect d'un des droits qui leur sont garantis. La Convention 108+ prévoit en outre que toute personne doit pouvoir « *bénéficier, quelle que soit sa nationalité ou sa résidence, de l'assistance d'une autorité de contrôle au sens de l'article 15 pour l'exercice de ses droits prévus par la présente Convention* ».[110]

[108] Rapport explicatif du protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données, STE 181, du 8 novembre 2001, point 5.
[109] Voir *infra*..
[110] Article 9, § 1, g, de la Convention 108+.

Ce droit à l'assistance des autorités de contrôle vise à assurer une protection effective des personnes concernées. Il sera particulièrement précieux dans les situations transfrontières, dans lesquelles la personne concernée réside dans un pays tandis que le responsable du traitement des données est établi dans un autre pays. Dans de telles circonstances, la personne concernée peut présenter sa demande par l'intermédiaire de l'autorité de l'État Partie dans lequel elle réside.

Cette hypothèse dans laquelle les personnes concernées relevant d'un autre État peuvent être efficacement aidées avait d'ailleurs été déjà envisagée en 1981 mais n'était pas formulée sous forme de droit et ne faisait pas encore intervenir les autorités de contrôle car celles-ci n'avaient pas leur place dans la Convention. L'article 14, § 1er de la version initiale de la Convention disposait ainsi que « *Chaque Partie prête assistance à toute personne ayant sa résidence à l'étranger pour l'exercice des droits prévus par son droit interne donnant effet aux principes énoncés à l'article 8 de la présente Convention* ». La formule de la Convention 108+ proposée sous forme de droit et ciblant précisément l'aide des autorités de contrôle est assurément plus percutante.

Ce droit peut être limité en application de l'article 11 ou aménagé pour préserver les intérêts d'une procédure judiciaire en cours[111].

VIII. – OBLIGATIONS COMPLÉMENTAIRES

Une disposition nouvelle, l'article 10*,* a été introduite dans la Convention modernisée pour ajouter aux obligations de transparence et de sécurité des obligations complémentaires.

Les Parties sont libres de moduler ces exigences en fonction de la nature et du volume des données, de la nature, de la portée et de la finalité du traitement et, le cas échéant de la taille des responsables du traitement et des sous-traitants[112]. Cette possibilité d'aménagement doit permettre d'éviter de mettre en place des obligations matérielles trop lourdes aux yeux de certains types de responsables de traitement, comme des « *petites et moyennes entreprises qui traitent uniquement des données à caractère personnel non sensibles reçues de consommateurs dans le cadre d'activités commerciales, et ne les réutilisent pas à d'autres fins* »[113].

A. – Accountability principle

Tout d'abord, il s'agit pour les responsables du traitement et, le cas échéant, les sous-traitants, de « *prendre toutes les mesures appropriées afin de se conformer aux obligations de la présente Convention et être en mesure de démontrer sous réserve de la législation nationale adoptée conformément à l'article 11, paragraphe 3, en particulier à l'autorité de contrôle compétente, prévue à l'article 15, que le traitement dont ils sont responsables est en conformité avec les dispositions de la présente Convention* »[114].

[111] Paragraphe 82 du Rapport explicatif de la Convention 108+.
[112] Article 10, § 4, de la Convention 108+.
[113] Paragraphe 90 du Rapport explicatif de la Convention 108+.
[114] Article 10, § 1er, de la Convention 108+.

C'est là une formulation succincte de ce qu'on a appelé l'*accountability principle*.[115] Il impose de mettre en place des mécanismes internes permettant de démontrer la conformité des traitements avec les dispositions applicables.

À titre d'exemples de mesures appropriées permettant aux responsables et aux sous-traitants de se mettre en conformité, le Rapport explicatif cite « *la formation des employés, la mise en place de procédures appropriées de notification (indiquant par exemple quand des données doivent être effacées du système), l'établissement de clauses contractuelles particulières en cas de délégation du traitement visant à donner effet à la Convention, ainsi que la mise en place de procédures internes permettant la vérification et la démonstration de la conformité* »[116].

C'est aussi comme mesure destinée à faciliter la vérification et la démonstration de la conformité des traitements de données qu'il est proposé que le responsable des traitements désigne un délégué à la protection des données disposant des moyens nécessaires à l'accomplissement de son mandat[117]. Le Rapport explicatif précise qu'il « *pourra s'agir d'un agent interne ou externe au responsable du traitement et sa désignation devra être notifiée à l'autorité de contrôle* »[118].

B. – *Examen de l'impact sur les droits et libertés fondamentales - obligation de minimisation des risques*

Avant de se mettre à traiter des données à caractère personnel, le responsable du traitement a l'obligation de procéder à un examen de l'impact de ce traitement de données sur les droits et libertés fondamentaux d'autrui et de concevoir le traitement de manière à minimiser cet impact. L'article 10, § 2, de la Convention 108+ dispose ainsi : « *les responsables du traitement, ainsi que, le cas échéant, les sous-traitants, doivent procéder, préalablement au commencement de tout traitement, à l'examen de l'impact potentiel du traitement de données envisagé sur les droits et libertés fondamentales des personnes concernées, et ils doivent concevoir le traitement de données de manière à prévenir ou à minimiser les risques d'atteinte à ces droits et libertés fondamentales.* » Lors de cet examen, le responsable du traitement est appelé à évaluer le respect du principe de proportionnalité à tous les stades envisagés du traitement de données et à aménager son traitement de données de façon à éviter les atteintes disproportionnées aux droits des personnes concernées[119].

---

[115] Le concept d'« *accountability* » n'est pas neuf et apparaît déjà dans les lignes directrices de l'OCDE du 23 septembre 1980 régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, article 14. Sur l'*accountability principle*, voir Groupe de l'article 29, Avis n° 3/2010 sur le principe de la responsabilité, WP 173 du 13 juillet 2010 ; G. BUTARELLI, « The accountability principle in the new GDPR », 30 September 2016, https://edps.europa.eu/sites/default/files/publication/16-09-30_accountability_speech_en.pdf.

[116] Paragraphe 85 du Rapport explicatif de la Convention 108+.

[117] Paragraphe 87 du Rapport explicatif de la Convention 108+.

[118] *Ibid.*.

[119] Paragraphe 88 du Rapport explicatif de la Convention 108+.

Cet examen[120] de l'impact sur les droits et libertés fondamentales peut être fait sans formalités excessives et avec éventuellement l'appui de développeurs de systèmes d'information, de spécialistes de la sécurité, de juristes ou d'usagers.

C. – *Prise en compte du respect de la vie privée dès la conception (Privacy by Design)*

Le principe de « *prise en compte de la vie privée dès la conception* » (*Privacy by Design*)[121] apparaît comme une exigence incontournable aujourd'hui pour réaliser efficacement la protection de la vie privée et des données. Cette exigence d'intégration de la préoccupation de protection de la vie privée au sein même des systèmes, produits et services créés et dès les premiers stades de leur conception permet d'offrir une protection effective à bien moindre frais que lorsqu'il faut intégrer les préoccupations de protection de la vie privée et des données par la suite, une fois le produit conçu et opérationnel.

L'article 10, § 3 de la Convention stipule dans cet esprit : « *Chaque Partie prévoit que les responsables du traitement, ainsi que, le cas échéant, les sous-traitants, prennent des mesures techniques et organisationnelles tenant compte des implications du droit à la protection des données à caractère personnel à tous les stades du traitement des données.* »

De telles mesures peuvent consister par exemple en « *un paramétrage par défaut favorable au respect de la vie privée de manière que l'utilisation des applications et logiciels ne porte pas atteinte aux droits des personnes concernées (protection des données par défaut), notamment afin d'éviter de traiter plus de données qu'il n'est nécessaire pour atteindre la finalité légitime. Par exemple, la configuration par défaut des réseaux sociaux devrait être telle que les messages ou les images ne soient partagés qu'avec un cercle restreint et choisi d'individus et non avec l'ensemble des internautes.* »[122] Ou encore, une configuration technique peut offrir une voie aisée pour l'exercice des droits. Ainsi, un accès sécurisé aux données en ligne devrait être proposé aux personnes concernées chaque fois que possible. Il devrait également y avoir des outils faciles à utiliser permettant aux

[120] Les auteurs de la modernisation de la Convention 108 ont veillé à ne pas reprendre la terminologie utilisée dans le RGPD qui évoque l'obligation de procéder à une « *analyse d'impact relative à la protection des données* » (article 35 RGPD). Cela, afin de ne pas associer l'examen de l'impact (issu de la Convention 108+) à une formalité systématiquement lourde, chère et contraignante, externalisée pour être réalisée par des spécialistes. Il se peut que l'examen des risques se présente comme tel, dans les cas de traitements de données complexes et de grande ampleur, par exemple, mais dans nombre de cas, il s'agira d'une démarche interne informelle de saine prise en considération des conséquences et risques liés au traitement de données projeté.

[121] Sur ce principe, voir A. CAVOUKIAN, « Operationalizing Privacy by Design : A Guide to Implementing Strong Privacy Practices », décembre 2012 ; B. PRENEEL et D. IKONOMOU (dir.), *Privacy Technologies and Policy: First Annual Privacy Forum*, *APF 2012*, Limassol, Cyprus, October 10-11, 2012, Revised Selected Papers, Berlin, Springer, 2014.

[122] Paragraphe 89 du Rapport explicatif de la Convention 108+.

personnes concernées de transférer leurs données à un autre fournisseur de service ou de conserver elles-mêmes les données (outils de portabilité des données)[123].

IX. – EXCEPTIONS

Comme signalé plus haut, des exceptions à certaines conditions de légitimité des traitements de données (à l'exigence de loyauté, au principe de finalité et à l'exigence de qualité des données) ainsi qu'à l'obligation de transparence (y compris la déclaration des incidents de sécurité que sont les violations de données[124]) et aux droits des personnes concernées, sont admises sous réserve de ce qui est dit à l'article 11 de la Convention 108+.

Ainsi, ces exceptions ne sont autorisées qu'à la condition[125] qu'elles soient prévues par la loi, qu'elles respectent l'essence des droits et libertés fondamentales et soient nécessaires, dans une société démocratique, à la protection d'intérêts supérieurs publics (a) ou privés (b) :

- (a) la sécurité nationale, la défense, la sûreté publique, des intérêts économiques et financiers importants de l'État, l'impartialité et l'indépendance de la justice, la prévention, l'investigation et la répression des infractions pénales et l'exécution des sanctions pénales, ainsi que d'autres objectifs essentiels d'intérêt public général ;

- (b) la protection de la personne concernée ou des droits et libertés fondamentales d'autrui, notamment la liberté d'expression.

Le Rapport explicatif rappelle que pour être considérée comme « *nécessaire dans une société démocratique* », une mesure doit poursuivre un but légitime et donc répondre à un besoin social impérieux qui ne peut être atteint par des moyens moins intrusifs. Cette mesure doit en outre être proportionnée au but légitime poursuivi et les motifs avancés par les autorités nationales pour le justifier doivent être pertinents et adéquats. Enfin, elle doit être établie par une loi accessible et prévisible qui doit être suffisamment détaillée[126].

X. – FLUX TRANSFRONTIÈRES DE DONNÉES

Avant la modernisation de la Convention 108, la question des flux transfrontières de données faisait l'objet de deux dispositions différentes, insérées l'une à l'article 12 de la Convention 108 (pour les flux transfrontières de données intra-Parties), l'autre dans le protocole additionnel de 2001[127] (pour les flux à destination de pays tiers à la Convention).

Les deux types de transferts de données à caractère personnel sont désormais abordés ensemble dans une seule disposition : l'article 14 de la Convention 108+.

---

[123] *Ibid.*.
[124] Voir *infra*.
[125] Article 11, § 1er de la Convention 108+.
[126] Paragraphe 91 du Rapport explicatif de la Convention 108+.
[127] Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données, STE n° 181, signé à Strasbourg le 8 novembre 2001.

Le régime des flux transfrontières vise à garantir que les données à caractère personnel entrant dans la juridiction d'une Partie à la Convention 108+ continuent d'être protégées avec des garanties appropriées lorsque, à la suite d'un transfert, elles tombent dans la juridiction d'un État non Partie. La protection offerte de l'autre côté de la frontière « *doit être d'une qualité suffisante pour garantir que l'internationalisation du traitement des données et les flux transfrontières de données n'aient pas de conséquences négatives sur les droits de l'homme* »[128].

A. – *Notion de transfert de données à caractère personnel*

On relèvera d'emblée que si la notion de flux transfrontières apparaît au niveau de l'intitulé de la disposition, il n'en est plus question ensuite. C'est la notion de « transfert » qui est présente dans l'énoncé des dispositions à ce sujet. Cette notion est précisée dans le Rapport explicatif de la façon suivante : « *Un transfert transfrontière de données intervient lorsque des données à caractère personnel sont communiquées ou mises à disposition d'un destinataire relevant de la juridiction d'un autre État ou d'une autre organisation internationale.* »[129] La notion de transfert couvre donc les situations comme la mise à disposition de données dans le *cloud* ou sur Internet, dans lesquelles, sans qu'il y ait véritablement de mouvement de données, ces dernières sont rendues accessibles à des personnes se situant au-delà des frontières.

B. – *Transfert de données entre Parties à la Convention 108+*

Les données à caractère personnel bénéficient de la liberté de flux entre Parties à la Convention[130]. Toutefois cette liberté n'est pas systématique, deux hypothèses de restriction des transferts de données sont envisagées par la Convention. Un État ou une organisation Partie pourrait, aux seules fins de la protection des données, interdire ou soumettre à une autorisation spéciale la communication ou la mise à disposition des données à un destinataire relevant de la juridiction d'une autre Partie à la Convention, dans l'hypothèse où :

- il existe un risque réel et sérieux que le transfert à une autre Partie, ou de cette autre Partie à une non-Partie, conduise à contourner les dispositions de la Convention ; pour invoquer cette exception il faut que la Partie originaire dispose de preuves claires et fiables que le transfert de données à l'autre Partie pourrait compromettre de manière significative la protection accordée aux données en question par la Convention et que la probabilité que cela se produise est élevée. « *Cela pourrait être le cas, par exemple, lorsque certaines protections prévues par la Convention ne sont plus garanties par l'autre Partie (par exemple parce que son autorité de contrôle n'est plus en mesure d'exercer efficacement ses fonctions).* »[131]

- l'État originaire doit respecter des règles de protection harmonisées communes à des États appartenant à une organisation internationale régionale. Il s'agit

[128] Paragraphe 103 du Rapport explicatif de la Convention 108+.
[129] Paragraphe 102 du Rapport explicatif de la Convention 108+.
[130] Article 14, § 1er, de la Convention 108+.
[131] Paragraphe 105 du Rapport explicatif de la Convention 108+

donc d'être soumis à la contrainte du respect de règles collectives et non de règles édictées individuellement et souverainement par l'État Partie. À titre d'exemple de règle harmonisée commune restreignant les flux entre certaines Parties, on peut citer le régime prévu au chapitre V du RGPD.

Par ailleurs, une Partie peut restreindre les transferts de données vers une autre Partie pour une autre fin que la protection des données. Un État peut par exemple interdire les transferts hors des frontières au nom de la sécurité nationale, la défense, la sûreté publique ou d'autres intérêts publics importants[132].

C. – *Transferts de données vers un État ou une organisation non Partie à la Convention 108+*

Pour les flux vers un destinataire relevant de la juridiction d'un État ou d'une organisation non Partie à la Convention, la règle est qu'ils ne sont autorisés que si un niveau approprié de protection fondé sur les dispositions de la Convention est garanti pour les données transmises[133]. On notera qu'à la différence du RGPD qui exige un niveau de protection « adéquat » pour permettre les flux de données à caractère personnel hors des frontières de l'Union européenne, la Convention réclame un niveau de protection « approprié ». Cette différence vise à éviter que le même terme ait deux significations différentes selon qu'il serait utilisé dans le contexte de l'Union européenne ou dans celui du Conseil de l'Europe.

Un niveau de protection approprié peut découler :

a) des règles de droit de l'État du destinataire ou de l'organisation internationale, notamment des traités ou accords internationaux applicables, ou

b) de garanties *ad hoc* ou standardisées agréées, établies par des instruments juridiquement contraignants et opposables, adoptés et mis en œuvre par les personnes impliquées dans le transfert et le traitement ultérieur des données (donc tant par la personne qui communique ou rend accessibles les données à caractère personnel que par le destinataire).

Il faut informer l'autorité de contrôle des mesures a*d hoc* ou standardisées prises pour assurer un niveau de protection des données approprié[134]. L'autorité n'a pas à donner son autorisation mais elle dispose du pouvoir de vérifier sur le terrain la qualité et l'effectivité des mesures prises et éventuellement d'interdire, suspendre ou conditionner un flux transfrontière.

Enfin, des exceptions sont prévues pour permettre de transmettre des données sans protection appropriée. C'est le cas :

- si la personne concernée a donné son consentement explicite, spécifique et libre, après avoir été informée des risques découlant de l'absence de garanties appropriées ; ou

[132] Paragraphe 105 du Rapport explicatif de la Convention 108+.
[133] Article 14, § 2 de la Convention 108+.
[134] Article 14, § 5 de la Convention 108+.

- si des intérêts spécifiques de la personne concernée le nécessitent dans un cas particulier ; ou

- si des intérêts légitimes prépondérants, notamment des intérêts publics importants, sont prévus par la loi et si ce transfert constitue une mesure nécessaire et proportionnée dans une société démocratique ; le Rapport explicatif[135] précise que, par cette exception, les données à caractère personnel peuvent être transférées pour des motifs similaires à ceux énumérés à l'article 11, de la Convention 108+ [136]; ou

- si ce transfert constitue une mesure nécessaire et proportionnée dans une société démocratique pour la liberté d'expression.

XI. – AUTORITÉS DE CONTRÔLE

En 1981 nul n'a songé à évoquer des autorités de contrôle spécifiques dans la Convention 108. Vingt ans plus tard, la volonté s'est fait jour de renforcer la protection effective de l'individu par le biais de la création d'une ou plusieurs autorités de contrôle qui contribuent à la protection des droits et libertés de l'individu à l'égard du traitement des données. L'expérience acquise durant ces vingt années a en effet démontré que lorsqu'elles sont dotées de compétences effectives et qu'elles jouissent d'une réelle indépendance dans l'exercice de leurs fonctions, de telles autorités sont devenues partie intégrante du système de contrôle de la protection des données dans une société démocratique.

Un protocole additionnel a donc été élaboré et adopté le 23 mai 2001 en vue d'ajouter au système de protection de 1981 une obligation à charge des États signataires de se doter d'une autorité de contrôle ayant pour mission de veiller, sur leur territoire, au respect de la réglementation de protection.

Vingt ans plus tard encore, un nouveau chapitre consacré aux autorités de contrôle transpose dans la Convention 108+, en les étoffant, les dispositions contenues à ce propos à l'article 2 du protocole additionnel de 2001.

L'article 15 vise en premier lieu à renforcer l'indépendance de ces autorités de contrôle, notamment en précisant que ces autorités doivent agir avec indépendance et impartialité dans l'accomplissement de leurs fonctions et l'exercice de leurs pouvoirs, sans solliciter ni accepter d'instructions de quiconque[137]. La garantie matérielle de l'indépendance a aussi été envisagée et le texte ajoute que les autorités de contrôle doivent disposer des ressources nécessaires à l'accomplissement effectif de leurs fonctions et à l'exercice de leurs pouvoirs[138].

---

[135] Paragraphe 108 du Rapport explicatif de la Convention 108+.
[136] Les motifs énumérés à l'article 11, § 1 sont la protection de la sécurité nationale, la défense, la sûreté publique, des intérêts économiques et financiers importants de l'État, l'impartialité et l'indépendance de la justice ou la prévention, l'investigation et la répression des infractions pénales et l'exécution des sanctions pénales, ainsi que d'autres objectifs essentiels d'intérêt public général ; la protection de la personne concernée ou des droits et libertés fondamentales d'autrui, notamment la liberté d'expression.
[137] Article 15, § 5 de la Convention 108+.
[138] Article 15, § 6 de la Convention 108+.

Le texte vise deuxièmement à renforcer les pouvoirs des autorités. Il reconnaît à cet effet que ces autorités doivent disposer de pouvoirs d'investigation et d'intervention, qu'elles sont compétentes en matière de flux transfrontières de données pour marquer leur agrément de clauses juridiques standardisées, qu'elles doivent pouvoir prononcer des décisions relatives aux violations des dispositions de la Convention et notamment sanctionner les infractions administratives, qu'elles disposent du pouvoir d'ester en justice, qu'elles sont chargées de sensibiliser et d'éduquer à la protection des données[139].

On relèvera que le renforcement le plus remarquable se situe au niveau du pouvoir de décision et de sanction autonome des autorités de contrôle. Par ailleurs, les autorités se voient confier une mission pédagogique en matière de protection des données, ce qui est assurément très pertinent si l'on prend en compte le contexte actuel dans lequel s'effectuent les traitements des données. La mission de sensibilisation et d'éducation devrait s'exercer à l'égard du public qu'il convient d'éveiller aux risques, qu'ils soient cachés ou non, issus des développements techniques et sociétaux. Mais il s'agirait aussi de sensibiliser les responsables de traitements sur les règles à respecter pour garantir un équilibre entre tous les intérêts en présence.

XII. – LE COMITÉ CONVENTIONNEL

Un Comité conventionnel aux fonctions renforcées va prendre le relais du Comité consultatif attaché à la Convention 108 initiale.

Il sera constitué d'un délégué par Partie et se voit attribuer une liste de fonctions allongée par rapport aux fonctions assumées par le Comité consultatif jusqu'à aujourd'hui[140]. Parmi ces fonctions figurent notamment : un pouvoir de recommandations en vue de faciliter ou d'améliorer l'application de la Convention, un pouvoir d'avis sur toute question relative à l'interprétation ou à l'application de la Convention ainsi que sur le niveau de protection des données à caractère personnel assuré par tout candidat à l'adhésion (avis pouvant être assorti de recommandations sur les mesures à prendre en vue d'atteindre la conformité avec les dispositions de la Convention) et un pouvoir d'examen régulier de la mise en œuvre de la Convention par les Parties et de recommandation des mesures à prendre en cas de non-respect de la Convention par une Partie. Ce dernier pouvoir d'examen est particulièrement important pour garantir la confiance entre Parties permettant de laisser sereinement les données circuler librement entre elles.

*
* *

Au terme de la présentation et de l'analyse de la Convention 108 modernisée, on soulignera les principaux atouts du nouveau texte.

[139] Article 15, § 2 de la Convention 108+.
[140] Article 23, a à i de la Convention 108+.

Il s'agit tout d'abord du seul instrument juridique contraignant à vocation universelle en matière de protection des données à caractère personnel. Cela permet d'offrir un modèle de régime de protection pour tous les États et organisations internationales préoccupés d'offrir des garanties aux individus dont les données font l'objet de traitements. Ce statut d'instrument universel présente en conséquence l'avantage que l'extension inexorable du nombre de Parties emporte un élargissement de la zone géographique dans laquelle les flux transfrontières de données sont en principe libres, hors l'application d'un régime régional spécifique.

En outre, le champ d'application de la Convention couvre toutes les activités d'une Partie, tant celles du secteur privé que celles du secteur public, et, parmi ces dernières, également les activités de traitements de données à caractère personnel dans le domaine de la sécurité nationale, la défense et la sûreté publique, moyennant bien sûr les aménagements et restrictions aux principes de protection nécessaires pour ne pas entraver l'efficacité de l'action des services.

Autre élément clé apporté par la révision de la Convention, la protection de la dignité humaine et de l'autonomie personnelle en présence de traitements de données à caractère personnel est soulignée dès le préambule du texte. Ce sont ces valeurs qui sont en jeu derrière les règles énoncées dans la Convention, en lien avec les droits et les libertés fondamentales des individus, tels le droit à la vie privée, la liberté d'expression et d'information, la liberté de mouvement, le droit à la non-discrimination, le droit à des élections libres, … La protection de ces valeurs de dignité et d'autonomie se traduit pour l'essentiel dans les droits garantis aux personnes concernées et les obligations pesant sur les responsables de traitements et leurs sous-traitants.

Une disposition est particulièrement importante dans la Convention 108+. Il s'agit de l'article 5, § 1, proclamant l'exigence de proportionnalité de tout traitement de données à caractère personnel. Le contrôle du respect de cette exigence permettra, le cas échéant, aux autorités de contrôle et aux juges de s'ériger en rempart contre des velléités de dérives qui mettraient à mal la dignité humaine ou se feraient au mépris des droits et libertés d'autrui en jeu.

Enfin, le renforcement du rôle du Comité conventionnel est particulièrement bienvenu. C'est son nouveau pouvoir d'examen de la mise en œuvre de la Convention préalablement à toute adhésion et également sous forme de suivi une fois la Convention ratifiée qui mérite d'être spécialement salué.